DET KONGELEGE FORNYINGS-
OG ADMINISTRASJONSDEPARTEMENT

Meld. St. 5

(2009–2010)

Melding til Stortinget

Datatilsynets og Personvernnemndas årsmeldingar for 2008

DET KONGELEGE FORNYINGS-
OG ADMINISTRASJONSDEPARTEMENT

Meld. St. 5

(2009–2010)

Melding til Stortinget

Datatilsynets og Personvernnemndas årsmeldingar for 2008

Innhald

DET KONGELEGE FORNYINGS-
OG ADMINISTRASJONSDEPARTEMENT

Meld. St. 5

(2009–2010)
Melding til Stortinget

Datatilsynets og Personvernnemndas årsmeldingar for 2008

Tilråding frå Fornyings- og administrasjonsdepartementet av 9. oktober 2009, godkjend i statsråd same dagen.
(Regjeringa Stoltenberg II)

1 Fornyings- og administrasjonsdepartementets innleiing

I eit samfunn med stort fokus på tryggleik og kontroll, blir tolegrensa for inngrep i den personlege sfæren stadig større. Overvaking og registrering har blitt ein del av kvardagen og høyrer i mange situasjonar til hovudregelen framfor unntaket. Mange reagerer ikkje på inngrep i deira personlege integritet i anna enn dei meir ekstreme tilfella.

Nettopp denne rutinen og aksepten av ein utstrekt bruk av integritetskrenkjande verkemiddel, gjer at det framleis er viktig å ha fokus på personvern. Trass i denne aksepten for at personvern av omsyn til «noko større» i mange tilfelle må setjast til side, har personvern fått stor merksemd i 2008. Media har følgt ei rekkje saker der retten har blitt krenkt eller står i fare for å bli krenkt. I 2008 har det vore spesielt fokus på personvern i skolen, manglande sletterutinar for og gjenbruk av personopplysningar og dessutan snoking i register. I tillegg fører eit teknologisk landskap under utvikling til stadig nye og vidtrekkande personvernutfordringar.Medvitet kring personvernproblematikken hos kvar enkelt har som følgje av bl.a. Datatilsynets arbeid, auka dei seinare åra. På grunn av det auka presset mot personvern, er òg eit auka medvit essensielt. Regjeringa har derfor framleis ei målsetjing om å auke medvitet blant befolkninga om dei truslar personvernet vert utsett for. I tillegg står det som eit mål å redusere personvernutfordringane til det som er strengt nødvendig. Regjeringa er oppteken av å utnytte den teknologiske utviklinga til både å finne personvernvennlege og personvernfremjande løysingar og vil derfor ha fokus på dette framover.

Datatilsynets og Personvernnemndas rapportar gir ein pekepinn om kva problem som har stått i fokus det siste året, og på kva område det trengst endringar. Nokre av dei problemområda det blir peikt på, er allereie under utbetring, mens det på andre område er behov for endringar. Regjeringa ønskjer å ha eit vedvarande fokus på personvern.

Personvernkommisjonen

Ut frå eit aukane press mot personvern på stadig nye område, blei Personvernkommisjonen oppnemnd 25.mai 2007. Rapporten blei fullført i løpet av 2008 og er teken inn i NOU 2009:1, Individ og integritet, som er sendt på høyring med høyringsfrist 20. august 2009. Rapporten gjer greie for gjeldande rett, og peiker på ulike personvernrelaterte utfordringar. Konkrete forslag til lovendringar er fremja i samanheng med etterkontrollen av personopplysningsloven og var ikkje innafor mandatet til kommisjonen. Kommisjonen gir ei overordna vurdering av personvernsitua-

sjonen i Noreg, men går i djupna berre på utvalde område som det har vore spesielt fokus på dei seinare åra.

Oppgåva til kommisjonen var å gi ein heilskapleg status over dei eksisterande personvernutfordringane, vurdere korleis ein bør ta vare på personvernet i møtet med motståande omsyn og verdiar, kartleggje og evaluere dei verkemiddel som i dag eksisterer for å ta vare på personvernet, fremje forslag til nye prinsipp og verkemiddel og samtidig vareta andre omsyn, i tillegg til å sjå på moglege tiltak og verkemiddel for betre etterleving av regelverket.[1]

Oppfølging av rapporten frå personvernkommisjonen

I etterkant av høyringsrunden vil regjeringa følgje opp rapporten, og vurdere tiltak for betre å vareta borgarane sitt personvern. Datatilsynet vil stå sentralt i dette arbeidet.

Regjeringa har allereie i 2009 sett av midlar til tiltak som inneber oppfølging av nokre av dei utfordringar som det vert peika på i rapporten. Midlane skal nyttast til å setje i verk tre prosjekt med utgangspunkt i Datatilsynet. For det første vil det bli sett i verk eit prosjekt med sikte på å heve kunnskap om personvern og å sikre ein betre internkontroll og informasjonstryggleik i norske verksemder. Dette inneber bl.a. ei satsing på personvernombodsordninga. Vidare er det sett av midlar til å setje i gang eit prosjekt vedrørande personvern i grunnskolen. Prosjektet skal gjennomførast i samarbeid mellom Kunnskapsdepartementet, Fornyings- og administrasjonsdepartementet og Datatilsynet. Målet er i første omgang å kartleggje dei utfordringar som ligg i skolesektoren, og vurdere korleis personvernet for elevar i grunnskolen kan styrkjast. Til slutt er det sett av midlar til å etablere ei teneste som skal bidra med hjelp til sletting av krenkjande personopplysningar på internett. Dette skal vere ei teneste som hovudsakeleg skal hjelpe til med rettleiingsarbeid for korleis ein kan forhindre slike krenkingar og korleis ein sjølv kan rette opp når skaden har skjedd. I første omgang blir det sett i verk som eit mellombels prosjekt, men dersom det viser seg å vere effektivt, tek ein sikte på å gjere ordninga permanent.

[1] NOU 2009:1 s. 12

Verksemders kunnskap og oppfylling av regelverket

Næringslivets Sikkerhetsråd (NSR) gjorde i 2008 ei mørketalsundersøking. Denne viste at ein høg prosentdel av verksemdene kjende til personvernregelverket. Mot 80 pst. av verksemdene som kjende til regelverket, var det berre 50 pst. som opplyste at regelverket blei etterlevd. Informasjonsarbeidet gjennomført av Datatilsynet har altså vore effektivt for å gjere verksemder merksame på det eksisterande regelverket. Når medvitet om regelverket er godt, gjenstår spørsmålet om kvifor det ikkje blir oppfylt i tråd med lovgivinga.

Ettersom dei fleste verksemder kjenner til regelverket, må hovudårsaka til brot på personvernlovgivinga vere manglande vilje og/eller evne til å gjennomføre dei tiltaka det er krav om. Datatilsynet peiker på moglege årsaker til at etterleving ikkje skjer; at dette er tidkrevjande, tek fokus bort frå kjerneoppgåver, kan krevje investeringar og gir lite direkte tilskot til botnlinja, i tillegg til at risikoen for at manglande etterleving blir oppdaga er relativt liten. Det er avgjerande at verksemder blir gjorde bevisste om dei langsiktige, positive effektane av å etterleve personvernreglementet og får eit sjølvstendig insentiv til å oppfylle forpliktingane.

Personvernkommisjonen peiker i si utgreiing, NOU 2009:1, på kor viktig det er at personvernmyndigheitene held seg oppdaterte på den teknologiske utviklinga, og nemner Datatilsynets faglege verksemd for å kartleggje og formidle teknologiutviklinga til politikarar og samfunn. Det blir peikt på eit behov for ei offentleg prioritering av å ruste opp brukarmiljø som handterer personopplysningar i riktig og effektiv bruk av bl.a. kryptering. At slike teknologiske personvernløysingar blir gjorde tilgjengelege, vil gjere det mindre krevjande for verksemder å oppfylle pliktene sine. Kombinasjonen mellom slike teknologiske løysingar, vedvarande informasjonsarbeid og kontroll, og ein utvida bruk av personvernombod, kan vere tiltak som medverkar til å forbetre oppfyllingsstatistikken. Regjeringa har derfor løyvd midlar til å setje i verk eit prosjekt som dreier seg om å få verksemder til å ta betre vare på personvernet.

Internasjonalt samarbeid

Spørsmål vedrørande personvern blir i stor grad påverka av internasjonale straumdrag. Den teknologiske utviklinga gjer det mogleg med fri flyt av informasjon på tvers av landegrensene. Det er

krevjande for brukarane å setje seg inn i og forstå konsekvensane av å gi frå seg personopplysningar på utanlandske nettstader. I tillegg oppstår det spørsmål om kva lands rett som regulerer forholdet. Den norske personopplysningsloven byggjer på EUs personverndirektiv, og byggjer derfor på dei same prinsippa som dei andre landa som har implementert direktivet. Konflikt vil likevel oppstå i møte med land som har eit svakare vern, slik som forholdet er i for eksempel Nord- Amerika.

Mykje av arbeidet retta mot personvern skjer på internasjonalt nivå. Det er viktig at Noreg deltek i forum der personvernutfordringar blir diskuterte og regelverk utarbeidd. Internasjonalt har det skjedd ei rekkje tiltak som vil kunne få konsekvensar for det nasjonale personvernet. Datalagringsdirektivet er eit døme på eit slikt internasjonalt grep som har blitt kritisert for å gripe for mykje inn i kvar enkelt sin rett til privatliv. Det er viktig at Noreg òg engasjerer seg i internasjonale fora for å få størst mogleg innverknad. På EU-nivå har Noreg rett til å ta del i arbeidsgrupper, slik som den såkalla artikkel 29 gruppa der Datatilsynet deltek som observatør. Arbeidet her er viktig for å vere førebudd på framtidige utfordringar mot personvernet.

Det er òg viktig at Datatilsynet tek del i den internasjonale arbeidsgruppa for personvern innan telekommunikasjon, den såkalla Berlin-gruppa, Spring Conference, Working Party on Police and Justice i tillegg til det nordiske samarbeidet. Regjeringa støttar eit vidare engasjement i det internasjonale arbeidet, og ønskjer ei personvernmyndigheit som er synleg på den internasjonale arena.

2 Fornyings- og administrasjonsdepartementets merknader til Datatilsynets årsmelding for 2008

Fornyings- og administrasjonsdepartementet har merka seg at Datatilsynet peiker på problem med manglande oppfylling av meldings- og varslingsplikta, plikta til internkontroll og informasjonstryggleik og dårleg oppfølging av sletteplikta. Fokus må rettast mot løysingar som bidreg til betre oppfylling av dei lovpålagde pliktene.

Ansvarsfråskriving og pulverisering av ansvar

Fokus blir retta først under kapittelet «Tema og tendensar i 2008» mot eit svekt personvern på grunn av ansvarsfråskrivingar. Datatilsynet rapporterer om ein tendens til pulverisering av ansvar som går på kostnad av den enkelte sitt personvern. Den behandlingsansvarlege skal ha det øvste ansvaret for at personvernkrenkingar ikkje skjer i samband med behandlinga av personopplysningar. Men i visse tilfelle viser det seg vanskeleg å fastsetje kven som er behandlingsansvarleg. Ei vedvarande auka medvit om personvern kan medverke til at verksemder får betre ansvarsrutinar.

Meir informasjon, større utveksling og utilstrekkeleg tryggleik

Manglande sletting og snoking i register er noko Datatilsynet har sett fokus på i meldingsåret. Det har blitt ein tendens til å lagre opplysningar lenger enn nødvendig, då det kostar mindre å lagre opplysningar enn å bruke tid på å sortere ut materiale som det ikkje lenger er nødvendig å oppbevare. Ei slik massiv lagring i kombinasjon med eit utilstrekkeleg vern mot snoking, utgjer ein monaleg trussel mot personvernet til den enkelte. Regjeringa støttar Datatilsynet i at det bør setjast inn tiltak for å forbetre sletterutinar og avgrense talet på personar med tilgang til personopplysningar som blir registrerte.

At det i tillegg er lagt opp til færre anonyme løysingar, sjølv når identifisering ikkje er nødvendig, medfører at betydelege mengder informasjon kan knytast til enkeltindividet. Regjeringa vil peike på at opplysningar berre skal lagrast i identifiserbar form dersom dette er nødvendig for det tilsikta formålet. I denne samanheng bør det arbeidast med tekniske løysingar som gjer enkle anonyme alternativ mogleg.

Når det skjer ei auka utveksling av data mellom ulike databasar og i tillegg ei utholing av teieplikta for å forenkle slik utveksling, vil eit større tal personar få tilgang til fleire personopplysningar. Dette fører med seg ein fare for at mange får ein god del overskotsinformasjon som dei ikkje har eit formålsmessig behov for. Oppbevaring av slik overskotsinformasjon vil vere i strid med personopplysningsloven.

Justissektoren

Det skjer ei omfattande behandling av personopplysningar innanfor justissektoren. Det finst ei rekkje register baserte på ulike heimelsgrunnlag, og politimyndigheitene har innsyn i atskillige register som høyrer til andre sektorar. Datatilsynet

uttrykkjer ei tydeleg bekymring for personverntilstanden i politisektoren.

Tilsynet gir først og fremst uttrykk for uro over utilstrekkeleg regulering av politiet sine register. Dei etterlyser klåre reglar for sletting og sanering, avklarte ansvarsforhold og ryddig rollefordeling for behandlinga av opplysningar, reglar for tilgangsstyring av databasar, klårgjering av teieplikta til politiet og ei avklaring av politiet sin tilgang til databasar hos andre aktørar.

Regjeringa la nyleg fram utkast til ny politiregisterlov. Forslaget inneber ei rekkje endringar samanlikna med rettstilstanden i dag. Den nye loven og tilhørande forskrift gjer klårare regler om behandlingsansvar, teieplikt, tilgang, innsyn, retting og sletting.

Datatilsynet har uttrykt sterk skepsis til at elektronisk lagring av fingeravtrykk no blir heimla i passloven. Dei har avdekt utilfredsstillende forvaltning av det eksisterande passregisteret, og er bekymra for tryggleiken forbunde med eit slikt utvida register som òg inneheld biometriske kjenneteikn. Regjeringa har etter grundige vurderingar bestemt seg for ikkje å foreslå lagring av fingeravtrykk i det sentrale passregisteret, jf. Ot. prp. nr. 64 (2008-2009) om endringar i passloven.

Det har vidare skjedd ei internasjonal utvikling når det gjeld utveksling av biometrisk informasjon. Ein slik auka utveksling av informasjon over landegrensene gjer det ytterlegare påkravd å sikre at biometrisk informasjon lagrast på ein sikker måte. Regjeringa har allereie i samband med DNA-reforma innført ei rekkje endringar i regelverket, blant anna etablering av etterforskingsregisteret for DNA-analysar og fleire andre endringar i påtaleinstruksen. Desse endringane bidrar til å sikre betre kontroll med opplysningar om DNA. Biometrisk informasjon vil i framtida vere omfatta av den nye politiregisterloven, noko som inneber at Datatilsynet vil føre tilsyn med registra.

Noreg har forhandla fram ei tilknytingsavtale til EU-regelverket om forsterka politisamarbeid (Prümbeslutnigane). Dette medfører at politiet får moglegheit til å søkje i EU-landa sine register, og at desse landa tilsvarande kan søkje i dei norske registra. Kontroll med at rette opplysningar lagrast i politiet sine databasar er derfor viktig. I dag er lagring av biometrisk informasjon heimla i straffeprosesslova og politiinstruksen, men vil i framtida regulerast i politiregisterlova, noko som utgjer eit betre rettsgrunnlag enn i dag.

Også datalagringsdirektivet vil kunne få stor tyding for justissektoren. Spørsmålet om implementeringa av direktivet har blitt vigd stor medieomtale i meldingsåret. Innføring av direktivet vil medføre at elektronisk kommunikasjon blir lagra i større omfang og over lengre tid enn i dag. Direktivet reiser viktige prinsipielle problemstillingar i forholdet mellom personvern og arbeidet mot kriminalitet. Frå regjeringa si side er det viktig at ein eventuell lovgiving om datalagring inneheld gode og sterke personvernreglar.

Internett

I meldingsåret har det vore eit sterkt press mot personvern på internett og innan telekommunikasjon. I media har det spesielt vore fokus på fildelingsspørsmålet. Datatilsynet nemner at konsesjonen til Advokatfirmaet Simonsen blei fornya i løpet av året, slik at dei framleis har høve til å loggføre IP- adresser. I etterkant av Datatilsynets årsmelding blei merksemda rundt fildelingsspørsmålet forsterka blant anna i samband med Pirate Bay-saka i Sverige, og «three strikes»-loven i Frankrike. Temaet reiser mange vanskelege spørsmål med personvernimplikasjonar. Det er nødvendig med ein offentleg debatt om korleis ein unngår at den enkelte sitt personvern blir sett til side samtidig som ein kan arbeide for å stanse slik ulovleg fildeling.

Datatilsynet har òg retta ein del av arbeidet sitt mot personvern i ulike nettsamfunn. I tillegg til at den som sjølv opprettar profil i nettsamfunnet publiserer ei rekkje opplysningar om seg sjølv, blir det lagt ut personopplysningar om andre aktørar. Datatilsynet har i denne samanhengen motteke mange førespurnader vedrørande kopiering og bruk av slike opplysningar i andre samanhenger. I denne samanheng har Datatilsynet foreslått at det blir oppretta ei hjelpelinje for personar som ufrivillig har fått krenkjande personopplysningar lagde ut på internett. Regjeringa har derfor gitt Datatilsynet midlar til å utgreie og opprette ei hjelpeteneste for personar som blir krenkte på internett.

Personvern hos barn og unge; internett og skole

Barn og unge er spesielt utsette for krenkingar på internett, eller dei står i fare for å utsetje andre for krenkingar. Det er avgjerande at desse gruppene får opplæring i fornuftig bruk av internett. Unge er svært aktive i nettsamfunn og er ofte meir kompetente enn føresette og lærarar i bruk av ny teknologi. Dei er likevel ikkje meir kompetente til å sjå og forstå kva konsekvensar bruk av nettet kan få for dei sjølve og andre, og kor langvarige slike

konsekvensar kan vere. Datatilsynets arbeid retta mot bruken av internett blant unge har vist seg å ha stor bevisstgjerande effekt. Du bestemmer-kampanjen hadde i 2007 stor verknad hos unge nettbrukarar. I meldingsåret blei det utarbeidd ein ny rettleiar om bilete av barn på internett. Denne var retta mot barnehagar, skolar og føresette for å forhindre at bilete av barn ukritisk blei lagde ut på nett.

Regjeringa ser positivt på dei initiativ Datatilsynet har teke for å betre personvernet hos barn og unge i skolen og på internett. Departementet ønskjer at det framleis skal arbeidast for bevisstgjering blant denne gruppa, og for å bevisstgjere føresette og barne- og ungdomsarbeidarar med omsyn til dei unges personvern. I NOU 2009: 1 er det peikt på ei rekkje behov for forbetringar når det gjeld personvern hos barn og unge.[2] I tillegg til dei behov barn har for vern mot krenkingar på internett, er det eit behov for å verne mot krenkingar i skolen. Personvernkommisjonen peiker på at barn har same rett til respekt for privatlivet som vaksne på arbeidsplassen, og at bl.a. skolens bruk av fjernsynsovervaking og overvakinga av PC-bruk reiser sentrale personvernspørsmål. Blant anna med bakgrunn i Personvernkommisjonens rapport skal det setjast i gang eit prosjekt som skal greie ut personvernsituasjonen i grunnskolen, og korleis ein best kan ta vare på barnas behov for vern. Personvernkommisjonen legg vekt på kor viktig det er å etablere samarbeid mellom sentrale aktørar innanfor skolesektoren. Prosjektgruppa vil bli sett saman i samarbeid mellom Datatilsynet, Kunnskapsdepartementet og Fornyings- og administrasjonsdepartementet. Det er nødvendig å inkludere både personvernmyndigheita og utdanningssektoren i arbeidet for å få best mogleg resultat.

Forsking og helse

Datatilsynet er bekymra for at helsepersonell har tilgang til overskotsinformasjon, og peiker på at dette er i strid med teieplikta. Det blei reagert på at det blir fremja forslag om å gi elektronisk tilgang til pasientjournal på tvers av verksemder då det, etter tilsynet si meining, ligg føre alvorlege manglar ved informasjonstryggleiken hos fleire av helseføretaka her i landet. Dersom det blir opna for tilgang på tvers av verksemdene, vil informasjon vere praktisk sett lettare tilgjengeleg for helsearbeidarar. Regjeringa påpeiker at ei slik ordning ikkje vil innebere fri tilgang til pasientjournalar for alle som jobbar i helsesektoren. På same måte som tidlegare har helsepersonell berre tilgang til den informasjonen dei har behov for i arbeidet sitt. Men dersom tilgangskontroll og tryggleiksrutinar sviktar, vil det kunne få større konsekvensar enn tidlegare. Det er derfor viktig at det skjer kvalitetskontroll med slike rutinar.

Tilsynsverksemd

Ein stor del av verksemda til Datatilsynet dreier seg om tilsyn og kontroll med etterleving av regelverket. Tilsyn blir gjennomførte med heimel i personopplysningsloven § 42 andre ledd nr. 3) hos behandlingsansvarlege i både privat og offentleg sektor. Tilsyna gir innsikt i utfordringane personvernet møter, set fokus på problemstillingar i ulike bransjar og avdekkjer brot på lovgivinga.

Det ligg likevel i dagen at det ikkje er mogleg for Datatilsynet å kontrollere alle tiltak som blir sette i verk. Det blei gjennomført 141 kontrollar i løpet av meldingsåret. Hovudfokus låg på elektronisk kommunikasjon og internett. Departementet er tilfreds med at Datatilsynet har ei omfattande tilsynsverksemd. Funna under kontrollen er derimot ikkje tilfredsstillande. Det blir diverre avdekt mange regelbrot, og brota er ofte knytte til meldings- og varslingsplikta, plikta til internkontroll og informasjonstryggleik, sletteplikta og oppfølgingsansvaret mot ekstern databehandlar. Det er derfor viktig å framleis ha merksemda retta mot betre etterleving av personopplysningsregelverket blant dei behandlingsansvarlege.

3 Fornyings- og administrasjonsdepartementets merknader til Personvernnemndas årsmelding for 2008

Dei sakene som har vore fremja for Personvernnemnda i meldingsåret, har hatt stor prinsipiell betyding. Sjølv om nemnda berre har myndigheit til å avgjere enkeltsaker, vil deira avgjerd ofte ha innverknad utover kvar enkelt sak. Det har blitt avsagt vedtak av prinsipiell betyding for bl.a. behandlinga av kredittopplysningar og for politiet sine register.

Personvernnemnda meiner ut frå vurderingane i sakene om kredittopplysningsbransjen, konkret selskapa Lindorff og Creditinform, at det bør skje ei forskriftsregulering av spørsmålet om kon-

[2] NOU 2009: 1 kap. 14

sesjon til kredittopplysningsfirma. Datatilsynet opererer med standardkonsesjon i slike tilfelle. Om denne praksisen for bruk av standardkonsesjon bør erstattast med ei forskriftsregulering, vil bli vurdert av regjeringa i samband med den pågåande etterkontrollen av personopplysningsloven.

Av sentral betydning er òg avgjerda om det sentrale straffe- og politiopplysningsregisteret (SSP). Nemnda etterlyser her ein rettspolitisk diskusjon av politiets registrering, oppbevaring, bruk og sletting av sensitive personopplysningar. Det er uttrykt spesiell bekymring for at det er vid tilgang til registeret, og manglande sletterutinar. Dei utfordringar nemnda peiker på i si saksbehandling vil finne si løysing i ny politiregisterlov, som regjeringa har oversendt Stortinget til behandling, samt dei nye datasystem som vil verte innført.

Verdt å nemne er også nemndas avgjerd om at ein utleigemeklar ikkje kan gjere kredittvurdering av kvar enkelt leigeinteressent. Nemnda godtok likevel at kredittvurdering av den som får tilbodet, skjer som ein siste sjekk. Departementet støttar Personvernnemnda i at det, i samsvar med gjeldande regelverk, bør vere ein viss terskel for å gjere kredittvurderingar.

4 Administrasjon og ressursar

Datatilsynets budsjett og rammevilkår

Datatilsynet hadde i 2008 eit budsjett i overkant av kr. 26 millionar. Vesentlege delar av dette går til å dekkje lønnskostnader. To millionar var øyremerkte kommunikasjonsprosjekt. På bakgrunn av det sterke presset personvern er sett under, er ein aktiv kommunikasjon med publikum viktig. Dette krev monalege 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 personopplysningsloven. Datatilsynet har fått mykje positiv merksemd om informasjonsarbeidet sitt, særleg arbeidet retta mot barn og unge. For å leggje til rette for at Datatilsynet skal kunne halde fram med det gode arbeidet, har Regjeringa auka tilsynets budsjett ytterlegare i inneverande år. Datatilsynet er tildelt midlar til tre nye prosjekt som no skal setjast i gang. Dette er dei nemnde prosjekta om oppretting av hjelpelinje for internettkrenkingar, personvern i skolen og informasjonstryggleik og internkontroll, irekna bruk av personvernombod, i norske verksemder.

Personvern er ikkje berre ei nasjonal sak. Særleg problemstillingar knytte til Internett, gir personvernarbeidet internasjonal dimensjon. Samarbeid med tilsynsmyndigheiter i andre land er derfor viktig. Datatilsynet deltek blant 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 bunden opp i reiseutgifter. Departementet deler Datatilsynets vurdering av at internasjonalt samarbeid er viktig, og støttar tilsynets prioritering i denne samanheng.

Personvernnemndas budsjett og rammevilkår

Personvernnemndas sekretariat består av ei deltidsstilling, og har i meldingsåret vore samlokalisert med Forbrukarrådet og Forbrukarombodet. Nemnda er fornøgd med sekretariatsordninga, og regjeringa meiner ordninga fungerer godt. Nemndas budsjett er i inneverande år på kr. 1,6 millionar.

Det er gjennomført 9 nemndmøte og eit tilsvarande tal saker er avgjorde. Saksmengda i Personvernnemnda har dei siste åra vore forholdsvis stabil, men sakene ser jamt over ut til å ha blitt meir komplekse og av meir prinsipiell art. Arbeidsmengda har derfor auka noko, trass i at talet på saker har vore stabilt. Det er viktig at Personvernnemnda også framover har ein beredskap for auke i tal på saker og/eller arbeidsmengd, slik at ein unngår lang saksbehandlingstid.

Ved utgangen av 2008 hadde leiar og nestleiar pluss to medlemmer av Personvernnemnda fungert i to periodar av fire år, og kunne dermed ikkje oppnemnast på ny. Det er viktig at Personvernnemnda gjennom sine arbeidsmetodar sikrar ein viss kontinuitet ved skiftet av leiing. Stortinget utnemnde hausten 2008 ny leiar og nestleiar av Personvernnemnda, og dei andre fem medlemmene av nemnda blei utpeikte av Fornyings- og administrasjonsdepartementet. I arbeidet med å finne nye nemndmedlemmer la Fornyings- og administrasjonsdepartementet 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 når Personvernnemnda blir sett saman.

Fornyings- og administrasjonsdepartementet

t i l r å r :

Tilråding frå Fornyings- og administrasjonsdepartementet av 9. oktober 2009 om Datatilsynets og Personvernnemndas årsmelding for 2008 blir send Stortinget

Vedlegg 1

Datatilsynets årsmelding for 2008

Del I

1 Om Datatilsynet

Datatilsynet ble etablert 1. januar 1980 som et uavhengig forvaltningsorgan, administrativt underordnet Fornyings- og administrasjonsdepartementet. Uavhengigheten innebærer at departementet ikke kan gi instruks om, eller omgjøre Datatilsynets utøving av myndighet etter personopplysnings- eller helseregisterloven. Personvernnemnda er klageinstans for Datatilsynets vedtak. Nemnda avgir sin egen årsmelding.

Oppgavene Datatilsynet ivaretar er fastsatt i Lov om behandling av personopplysninger av 14. april 2000 (personopplysningsloven) og Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) av 18. mai 2001.

Datatilsynet har til oppgave å beskytte den enkelte mot at personverninteressene krenkes gjennom behandling av personopplysninger. Personopplysninger skal behandles i samsvar med grunnleggende personvernhensyn, som vern av personlig integritet og privatlivets fred. I tillegg skal Datatilsynet holde seg orientert og informere om den nasjonale og internasjonale utviklingen i behandlingen av personopplysninger, og om de problemene som knytter seg til slik behandling. Datatilsynet skal identifisere farer for personvernet og gi råd om hvordan de kan unngås eller begrenses, og bidra som høringsinstans i saker som kan ha en personvernmessig konsekvens. Videre er deltakelse i råd og utvalg en viktig del av Datatilsynets arbeid.

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

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

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

2 Organisasjon og administrasjon

Datatilsynets budsjett og rammevilkår

Datatilsynets budsjett var i 2008 på i overkant av 26 millioner kroner, en økning på én million fra året før. To millioner kroner var øremerket kommunikasjonsprosjekt. I tillegg fikk Datatilsynet en belastningsfullmakt fra Fornyings- og administrasjonsdepartementet på ytterligere 1,1 millioner kroner for et kunstprosjekt og et filmprosjekt i tilknytning til «Du bestemmer». Det er opprettet to nye stillinger i tilsyns- og sikkerhetsavdelingen som følge av budsjettøkningen. Ca 66 % av det samlede budsjettet går til lønnskostnader, fordelt på 35 medarbeidere. Ut over kommunikasjonsprosjektet er det lite rom for å sette i gang tiltak som ikke direkte knytter seg til juridisk saksbehandling eller tilsynsvirksomhet.

Datatilsynet ble i 2008 tildelt ITAKT-prisen. ITAKT-prisen tildeles til personer eller virksomheter som har utmerket seg når det gjelder kriminalitetsbekjempelse innen telekommunikasjons- og internettsektoren. Datatilsynet fikk ett kunstverk og 20 000 kroner.

Som tilsynsorgan skal Datatilsynet dekke hele landet, inklusive Svalbard, og gjennomføring av tilsyn medfører en del reisevirksomhet.

Organisasjon

Datatilsynet var i 2008 bemannet med 35 årsverk, som fordeler seg slik:

- Direktøren
- Juridisk avdeling: 12 medarbeidere
- Tilsyn- og sikkerhetsavdelingen 7 medarbeidere
- Administrasjonsavdelingen 7 medarbeidere
- Informasjonsavdelingen 8 medarbeidere. Fire av disse er jurister knyttet til Datatilsynets juridiske svartjeneste, Frontservice. Frontservice betjener henvendelser per telefon og e-post ved siden av ordinær saksbehandling.

Datatilsynet vurderer kjønnssammensetningen fortløpende og søker å ta hensyn til å rekruttere i forhold til denne om kvalifikasjonene ellers er like. To kvinner har hele eller deler av virksomhetsåret hatt svangerskapspermisjon.

Datatilsynet har som mål å arbeide aktivt for at etaten til enhver tid gir kvinner og menn like arbeidsforhold og like muligheter til karriereutvikling og faglig utvikling. Gjennomsnittsalderen i Datatilsynet er for tiden 42 år for menn og 39 år for kvinner.

To medarbeidere sluttet i virksomhetsåret.

Datatilsynet ønsker å stimulere til et kulturelt og kompetansemessig mangfold i staben. Videre tilrettelegges det for en personalpolitikk som skal virke motiverende, og hindre utstøting av personer med nedsatt funksjonsevne. Datatilsynet er knyttet til avtalen om inkluderende arbeidsliv. Fokus har også i 2008 vært tiltak som forebygger belastningslidelser. Dette har vært tiltak knyttet til trening, ergonomisk veiledning og instruksjon om hensiktsmessig arbeidsteknikk.

3 Saksbehandling

Det ble journalført totalt 7164 dokumenter i meldingsåret. Av disse var 3882 innkomne og 3010 utgående brev fra Datatilsynet. Resten var journalførte interne notater. Dette er omtrent på samme nivå som for 2007.

Nye saker (som ikke har startet i et tidligere meldingsår) utgjorde 2048, hvorav 1315 ble fordelt til juridisk avdeling, mens 411 og 228 saker ble fordelt henholdsvis til Datatilsynets juridiske svartjeneste og tilsyns- og sikkerhetsavdelingen. Resten av sakene ble fordelt til administrasjonen, informasjonsavdelingen og direktøren.

Konsesjoner

I meldingsåret ble det gitt 206 konsesjoner for behandling av (sensitive) personopplysninger. Av disse utgjorde bruk av personopplysninger i forskning godt over halvparten av søknadene. I årsmeldingen for 2006 og 2007 ble det redegjort for konsekvensene i tilknytning til ny forskningslov. Det er ventet at Datatilsynet vil se en merkbar nedgang i antallet konsesjonssøknader når loven er i kraft. Forskningsloven vil, etter det som er kjent i skrivende stund, tre i kraft tidligst 1. juli 2009.

Andre tillatelser verdt å nevne er konsesjoner knyttet til frivillig dopingkontroll på treningssentre, samt kartlegging av boforhold for vanskeligstilte i kommunene.

Meldeplikten

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

I 2008 kom det inn 2910 nye meldinger om behandling av personopplysninger mot 2952 i 2007. Totalt er det nå 8640 meldinger i meldingsdatabasen, mot 8946 året før. Det har med andre ord vært en liten nedgang i antallet meldinger. Noe av nedgangen skyldes antagelig at en del virksomheter som har opprettet personvernombud ikke lenger er meldepliktige til Datatilsynet. 3212 meldinger ble i meldingsåret slettet fra databasen som utløpt på dato i forhold til treårsregelen, mot 2989 året før.

Klagesaker til Personvernnemnda

I meldingsåret oversendte Datatilsynet sju saker til Personvernnemnda for videre klagebehandling: Dette gjaldt:

- Klage på Datatilsynets avgjørelse vedrørende praksis med kredittvurdering av potensielle leietakere
- Sletting av opplysninger i Det sentrale straffe- og politiregister SSP
- Klage over deler av vedtak etter kontroll hos OBOS-megleren – bruk av eMegler
- Klage på kategorisering som ikke kredittverdig hos Lindorff Decision – bruk av adressehistorikk
- Klage på bransjeanalyse for CreditInform AS
- Klage på Datatilsynets avvisningsvedtak – Gjenoppretting av pasientjournal

Samtlige saker ble avgjort i meldingsåret og Datatilsynet fikk medhold i tre av sakene.

For nærmere redegjørelse om de konkrete sakene viser Datatilsynet til Personvernnemndas årsmelding. Datatilsynet vil likevel bemerke at tre av sakene er knyttet til bruk av kredittopplysninger. Klager fikk medhold i to av disse sakene.

Datatilsynet vil i tillegg trekke frem vedtaket knyttet til sletting i Det sentrale straffe- og politiopplysningsregisteret. Her fikk Datatilsynet medhold. Saken har etter tilsynets oppfatning stor prinsipiell betydning, i det Personvernnemnda uttaler seg om grensene for Datatilsynets kompetanse i forhold til rettspleielovene.

I meldingsåret mottok Datatilsynet i tillegg vedtak i tre saker som var oversendt Personvernnemnda i 2007. Dette gjaldt:

– Klage på vedtak om krav om samtykke for registrering i historisk database – Biblioteksystemer
– Klage på avvisningsvedtak – innsyn i personopplysninger hos OBOS
– Klage på vedtak om bruk av fødselsnummer på www.ung1881.no

I samtlige av disse tre sakene ble Datatilsynets vedtak stadfestet.

Datatilsynet vil bemerke at det ikke bør legges stor vekt på antallet vedtak som blir omgjort eller opprettholdt av Personvernnemnda uten at man samtidig ser hen til det store antallet vedtak som aldri blir påklaget. Datatilsynets erfaring er at de saker som blir oversendt til Personvernnemnda ofte knytter seg til områder der lovgivningen er uklar, og hvor klager, så vel som Datatilsynet, ser seg tjent med å få en avgjørelse fra Personvernnemnda som klargjør rettstilstanden. En annen kategori saker er vedtak som oppleves som begrensende for den klageren, men hvor han likevel velger å påklage, til tross for at rettstilstanden er relativt avklart.

Saksbehandling i tilknytning til internasjonale fora

Datatilsynet mottar en rekke forespørsler og spørreundersøkelser fra artikkel 29-gruppen og de andre internasjonale fora tilsynet deltar i. I tillegg kommer en del henvendelser direkte fra de andre europeiske tilsynsmyndighetene. Datatilsynet har i meldingsåret registrert ca 30 henvendelser fra andre land med spørsmål, samt mottatt fem til dels omfattende spørreskjemaer knyttet til forskjellige felt. Disse spørsmålene og spørreskjemaene bevares i hovedsak uformelt via e-post. Datatilsynet noterer at dette beslaglegger en god del ressurser. Det er imidlertid Datatilsynets oppfatning at det er viktig å behandle denne typen henvendelser, i det de bidrar til en felles forståelse og håndhevning av direktivet i Europa. De er også viktige kanaler for utveksling av erfaringer og kunnskap. Datatilsynet benytter selv disse kanalene for å kartlegge hvordan problemstillinger løses av våre søsterorganisasjoner, særlig dersom reglene er uklare i Norge, eller der den behandlingsansvarlige er etablert i flere land. I meldingsåret har Datatilsynet ved to anledninger benyttet artikkel 29-gruppens e-postliste for å innhente synspunkter fra samtlige av de andre tilsynsorganene. Begge sakene hadde tilknytning til behandling av personopplysninger i virksomheter med stor aktivitet i en rekke land både innen og utenfor EU/EØS-området. Svarene var til god hjelp i saksbehandlingen.

Fra artikkel 29-gruppens side har det vært lagt ned mye arbeid for å finne effektive metoder for å håndtere virksomheter som vil opprettet bindende konsernregler (BCR) for utlevering av personopplysninger til utlandet. I dag behandles disse etter et komplekst system der alle landene kontrollerer om reglene tilfredsstiller de nasjonale kravene til utlevering av personopplysninger. Datatilsynet har blitt med i en prøveordning der man i større grad aksepterer at det land der virksomheten har sitt hovedsete kontrollerer lovligheten av BCR på vegne av de øvrige, berørte tilsynsmyndighetene. Dette er en løsning som på sikt kan spare Datatilsynet for mye arbeid, samtidig som personvernet synes godt ivaretatt.

Personvernombud

Datatilsynet har, ved utgangen av meldingsåret, registrert 124 personvernombud som til sammen representerer over 300 virksomheter. Fokus i 2008 har vært å kvalitetssikre ordningen i forhold til eksisterende ombud. Veksten i antall ombud har vært noe lavere i 2008 sammenlignet med de siste par årene. Datatilsynet har likevel holdt tre foredrag om ordningen basert på invitasjoner fra virksomheter. Av de nye ombudene er det spesielt gledelig at offentlige etater som Arbeids- og inkluderingsdepartementet, Brønnøysundregistrene, Kystverket og Landbruks- og matdepartementet har valgt å implementere ordningen i sin virksomhet.

Datatilsynet arrangerte fire kurs for personvernombudene i 2008. To av kursene var for nye personvernombud. Opplæringskursene tar for

seg internkontroll og sentrale begrep i personopplysningsloven. I tillegg gjennomgås rollen som personvernombud, og hvilke krav Datatilsynet stiller til ombudene. Det årlige seminaret for ombudene ble arrangert i mai, og oppslutningen var god. Etter et kort fellesprogram ble det holdt fem parallelle sesjoner for henholdsvis kommune/utdanning, personal/arbeidsliv, bank, inkasso og helse. Datatilsynet arrangerte også et eget seminar hvor temaet var informasjonssikkerhet.

4 Deltakelse i offentlige råd og utvalg

Datatilsynet skal bidra til å fremme respekten for det enkelte samfunnsmedlems privatliv, særlig når det gjelder bruk av personopplysninger. Råd- og utvalgsarbeidet er et viktig middel for å nå dette målet.

I meldingsåret har Datatilsynet deltatt i følgende råd og utvalg:

Arbeidsgruppe – lagring av elektronisk spormateriale

Arbeidsgruppen ble nedsatt av Politidirektoratet for å kartlegge dagens regelverk og praksis med hensyn til sikring av elektroniske spor etter at det foreligger rettskraftig dom. I tillegg skal gruppen foreslå hensiktsmessige løsninger for lagring. Gruppen besto av deltagere fra Politidirektoratet, Økokrim, KRIPOS, Oslo politidistrikt, Riksarkivet og Datatilsynet. Det ble avholdt totalt syv møter i tiden fra august til desember. Arbeidsgruppen avleverte sin rapport til Politidirektoratet medio desember. Arbeidsgruppen konkluderer med at det ikke er behov for å lagre elektronisk spormateriale som ikke inngår i straffesaken. Derimot er det behov for å sikre notoritet i behandlingen av det som inngår i straffesaken i alle ledd i straffesakskjeden, samt etablere overordnede rutiner for oppbevaring og lagring av spormateriale for eventuell senere bruk. Konkret påpekes behovet for å bruke lydopptak av alle rettsforhandlinger og regler for lagring av disse. Arbeidsgruppen går for øvrig av sikkerhetsmessige årsaker inn for sentralisert lagring av de elektroniske spor som besluttes lagret. Datatilsynet deltok med en jurist.

Arbeidsgruppe for opprettelse av Offentlig elektronisk postjournal (OEP)

Gruppen ledes av Fornyings- og Administrasjonsdepartementet. Gruppens arbeid har vært satt på vent i 2008 grunnet at lov og forskrift ikke var vedtatt. Reglene ble vedtatt senhøstes 2008 og reglene om OEP er i kraft fra 1. juli 2009. Arbeidet forventes å bli avsluttet innen den tid.

Samarbeidsråd for helsesektoren

Rådet er opprettet av Sosial- og Helsedirektoratet med sikte på å koordinere arbeid med informasjonsteknologi i helsesektoren. Formålet med rådet er å styrke samarbeidet aktørene imellom og med de sentrale myndigheter. Datatilsynet oppfatter rådet som et viktig forum, og deltar som observatør.

Bransjenorm for helsesektoren

Sosial- og Helsedirektoratet har gjennomført et større prosjekt hvor formålet var å utvikle en bransjenorm for helsesektoren. Normen skal bidra til å harmonisere nivået i helsesektoren hva gjelder informasjonssikkerhet. Datatilsynet har bistått med råd og veiledning ved utforming av normen. Arbeidet med normen ble avsluttet september 2006, men det utvikles stadig tilhørende faktaark som utdyper normen. En styringsgruppe, som Datatilsynet deltar i, har overtatt ansvaret for forvaltning av normen. Arbeidet består nå i å få en hensiktsmessig spredning og implementering av normen i sektoren. Dette skaper store utfordringer gitt sammensetningen av små, mellomstore og store aktører.

I meldingsåret deltok Datatilsynet i arbeidet med å utforme to veiledere.

1. *Veileder for kommuners tilknytning til helsenett.* Veilederen gir førende anbefalinger og råd om hva som må ivaretas av gjeldende tekniske og administrative krav til informasjonssikkerhet når en kommune eller fylkeskommune tilnyttes helsenettet.
2. *Veiledning i informasjonssikkerhet for forskning* Veilederen bygger på den nye helseforskningsloven med forskrifter, og er utarbeidet i samarbeid med representanter fra sektoren.

KIS – Koordineringsutvalget for informasjonssikkerhet

Utvalget består av representanter for sju departementer, Statsministerens kontor og ni direktorater. Opprettelsen av koordineringsutvalget er et ledd i gjennomføringen av Nasjonal strategi for informasjonssikkerhet. Arbeidet omfatter alminnelig IT-sikkerhet og spørsmål knyttet til rikets sik-

kerhet, vitale nasjonale sikkerhetsinteresser og kritiske samfunnsfunksjoner. Utvalget skal samordne videreutviklingen av IT-sikkerhetsregelverket, få frem felles standarder, normer, metoder og verktøy for IT-sikkerhet og sørge for samordning av tilsynspraksis. Utvalget skal også drøfte aktuelle risiko- og sårbarhetsspørsmål og bidra til koordinering av informasjonstiltak og beredskapsplanlegging. Mye av arbeidet i KIS delegeres til arbeidsgrupper. Datatilsynet har prioritert å være aktiv i disse arbeidsgruppene.

KOBI – begrepsapparat innen regulering av informasjonssikkerhet

Koordineringsutvalget opprettet KOBI som en ny gruppe i 2006. Alle myndigheter som regulerer informasjonssikkerhet sitter i denne gruppen. Siktemålet er å lage en metode for klassifisering av informasjon med utgangspunkt i behovet for beskyttelse.

Koordineringsutvalget for E-forvaltning

Utvalget skal arbeide med samordning mellom forskjellige offentlige organer for å realisere IT-politisk plan. Møtene ledes av Fornyings- og administrasjonsministeren. Arbeidet fokuserer på hvordan målene i planen kan realiseres, og hvordan de enkelte aktørene kan bidra.

NAFAL

NAFAL er et tilpasningsråd for sivil luftfart. Hovedtemaet i rådet er implementering av sikkerhetsløsninger på flyplasser. Innen denne tematikken reises en rekke spørsmål i forhold til personvern.

5 Internasjonalt samarbeid

I likhet med deltakelse i norske offentlige råd og utvalg, er også deltakelse på internasjonale møter og arbeidsgrupper en viktig arena for å påvirke personvernutviklingen. EU er den viktigste premissleverandøren for fremtidige personvernrettslige normer og regler. Datatilsynet har derfor valgt å være deltaker i utvalgte arbeidsgrupper under artikkel 29-gruppen. De internasjonale møtene er også en arena for utveksling av synspunkter. Nedenfor er en oversikt over de internasjonale arbeidsgrupper og råd som Datatilsynet er representert i.

Artikkel 29-gruppen

Den norske personopplysningsloven reflekterer personvernprinsippene som er nedfelt i EU-direktivet om personvern. Datatilsynet deltar som observatør i arbeidsgruppen opprettet etter direktivets artikkel 29. Gruppen har som oppgave å drive frem koordinering og synkronisering av EU/EØS-landenes nasjonale personvernarbeid, med utgangspunkt i personverndirektiv 46/95. Gruppen har en rådgivende funksjon overfor Kommisjonen og står fritt til å tolke og konkretisere direktivets innhold. I løpet av meldingsåret avholdt gruppen fem møter i Brüssel. Datatilsynet deltok på samtlige møter med direktøren, samt en saksbehandler i tillegg på tre møter.

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

- *Medical Data.* Arbeidsgruppen har hovedfokus på helsejournaler. Datatilsynet har deltatt på ett møte i 2008.
- *Technology subgroup (tidigere Internet task force)*. Arbeidsgruppen arbeider med internettrelaterte spørsmål, med vekt på det tekniske. Datatilsynet har deltatt på to møter.

Berlin-gruppen

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

- Bruk av «svarte bokser» i kjøretøy. Hvilken informasjon lagres og hvordan benyttes slike data?
- Lagring av innhold i SMS for lovhåndhevelse.
- Utvikling og bruk av PET-teknologi.
- Personvern i sosiale nettverk.
- Veiprising og personvern.
- Digitale rettigheter – hvordan ivareta personvernet.

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

Spring Conference

Hver vår avholdes et større «vårmøte» der artikkel 29-gruppen inviterer tilsynsmyndigheter fra land som ikke er del av EU/EØS, som for eksempel Sveits. Møtet ble i år arrangert i Roma. Datatilsynet deltok med direktøren og en saksbehandler.

Working Party on Police and Justice

Gruppen arbeider med spørsmål vedrørende politisamarbeid som faller inn under tredje søyle, det vil si utenfor det indre marked. Gruppen rapporterer til Spring Conference og eventuelle forslag og resolusjoner vedtas her. I 2008 arbeidet gruppen blant annet med forhold knyttet til Lisboa-avtalen, samt spørsmål om behandling av personopplysninger i tilknytning til Cybercrime-konvensjonen. Datatilsynet er representert med en saksbehandler. Det er avholdt tre heldagsmøter i meldingsåret.

Joint Supervisory Authority

JSA er det felles tilsynsorganet for Schengen Informasjonssystem (SIS). Informasjonssystemet inneholder opplysninger om personer som er ettersøkt, savnet, nektet innreise til Schengen-området, eller er straffedømt i et av medlemslandene. Møtene avholdes normalt i tilknytning til møtene i Working Party on Police and Justice i Brüssel, og Datatilsynet er representert med ett medlem i gruppen. I tillegg har en informasjonsmedarbeider bistått i arbeidet med å utvikle informasjonsmateriell knyttet til innføringen av SIS II.

Kontrollkommisjonen for Interpol

Datatilsynets representant i JSA er oppnevnt som vararepresentant i kontrollkommisjonen for Interpols register. Kommisjonen skal bistå i arbeidet med å sikre den enkeltes rettigheter i tilknytning til behandling av opplysninger om dem hos Interpol. Kommisjonen skal overvåke anvendelsen av personvernlovgivning innen dette området, samt behandle forespørsler om innsyn i Interpols registre. Vervet har medført deltagelse på to heldagsmøter i Lyon i meldingsåret.

Det internasjonale datatilsynssjefsmøtet

Hvert år holdes det en internasjonal konferanse for datatilsynssjefer med deltakere fra hele verden. Konferansen inneholder en åpen del som også andre enn datatilsynssjefene kan delta på. I 2008 ble konferansen holdt i Strasbourg, Frankrike. Datatilsynet deltok med direktøren, informasjonsdirektøren og en saksbehandler.

Internasjonalt saksbehandlermøte

Dette er et internasjonalt samarbeidsforum for juridiske saksbehandlere. Det ble avholdt to møter, henholdsvis i Ljubljana og Bratislava. Diskusjonene omhandlet blant annet behandling av personopplysninger på Internett og bruk av biometri. I tillegg har temaer som personvern kontra ytringsfrihet og behandling av personopplysning i løsninger for varsling i arbeidslivet stått på agendaen. Datatilsynet var representert med to saksbehandlere på disse møtene.

Nordisk datatilsynsjefmøte

Dette er et møte for direktørene i de nordiske datatilsynene, og arrangeres annet hvert år. I meldingsåret er det ikke avholdt møte.

Nordisk saksbehandlermøte

Dette er et årlig nordisk forum for saksbehandlere. Arrangementet ble i 2008 avholdt i Stockholm. Møtet hadde særlig fokus på kameraovervåking, som følge av at man i Danmark hadde innført en ny lov om privat kameraovervåking. Disse møtene er ellers et viktig forum for utveksling av erfaringer mellom de nordiske landene. Datatilsynet var representert med tre saksbehandlere.

Nordisk teknologimøte

Det ble avhold et møte i Oslo hvor det var deltakere fra øvrige Datatilsyn i Norden. Blant de sentrale spørsmål som ble drøftet var:
- Datalagringsdirektivet
- Tekniske funn på kontroller
- Google
- Sikkerhet ved Facebook
- e-billettering og RFID
- e-ID, elektroniske signaturer og nettbanker
- Pass og fingeravtrykk
- Nettbanker og e-faktura.

6 Informasjonsvirksomheten

2008 har vært et meget aktivt år når det gjelder informasjonsarbeidet. Personvernmyndighetene

har, også internasjonalt, fått en stadig større forståelse for at ivaretakelsen av personvernhensyn er avhengig av at tilsynsmyndighetene ikke ensidig satser på juridiske virkemidler, tilsynsvirksomhet og sanksjoner. Det er helt avgjørende å skape oppmerksomhet, og få til en aktiv debatt, refleksjon og bevissthet om personvernspørsmål. Selv om Datatilsynet, i større grad enn mange andre lands personvernmyndigheter, alltid har lagt stor vekt på sin informasjonsvirksomhet, så har dette virkemiddelet fått en stadig større betydning også her hos oss. En stor andel av medarbeiderne er blitt rustet til å kunne gi uttalelser innen egne saksområder til media, skrive kronikker og holde foredrag. På denne måten har Datatilsynet, sett i forhold til organisasjonens beskjedne størrelse, utviklet en meget stor kapasitet til å kunne tale personvernets sak så snart anledningene byr seg.

Datatilsynet høstet i 2008 flere anerkjennelser for sitt kommunikasjonsarbeid. I april ble kommunikasjonsbransjens fagpris tildelt Datatilsynet. Prisen deles ut av Norsk kommunikasjonsforening og Norske Informasjonsrådgivere (NIR) i fellesskap. Prisen gir honnør til kommunikasjonsbransjens egne utøvere av faget som har gjort et fremragende stykke kommunikasjonsarbeid/PR-kampanje. Utmerkelsen begrunnes med Datatilsynets langsiktige og målrettede arbeid innen sitt fagfelt. Videre ble direktør Georg Apenes i august tildelt Computerworlds hederspris for sin lange og iherdige innsats for personvernets stilling i Norge. I november ble han også tildelt Rosing-Akademiets Hederspris 2008. Prisen deles ut av Dataforeningen.

Datatilsynet tillater seg å tolke dette samlet sett som uttrykk for at kommunikasjonsvirksomheten utøves på en målrettet og profesjonelle måte.

Som det også fremgår nedenfor har de øremerkede ekstramidlene fra Fornyings- og administrasjondepartementet til ekstra satsing på kommunikasjonstiltak dermed gitt synlige og dokumentert gode resultater.

Undervisningsopplegget «Du bestemmer»:

Undervisningsopplegget «Du bestemmer» er utviklet i samarbeid med Teknologirådet og Utdanningsdirektoratet, og ble lansert januar 2007. Opplegget retter seg primært mot ungdom på 14-16 år, og handler om hvordan man kan ta kontroll over egne personopplysninger, og respektere andres integritet. Ved utgangen av 2008 var det til sammen sendt ut 7 341 klassesett på bakgrunn av bestillinger fra skoler og andre. Dette utgjør over 220 000 brosjyrer.

Filmproduksjon

Basert på den positive mottakelsen av undervisningsopplegget og tilbakemeldinger fra skoler og elever om at man ønsket mer film som diskusjonsgrunnlag, ble det besluttet å la ungdom selv lage filmer. Det ble derfor utlyst en manuskonkurranse med personvern og digitale medier som tema. Juryleder Harald Zwart plukket ut vinnermanusene. Seks vinnerteam fordelt på videregående skoler fra hele landet fikk hjelp fra profesjonelle filmfolk til å arbeide med utvikling av manus og filmproduksjon. I mars 2008 hadde filmene premierevisning på Filmens Hus.

Datatilsynet gikk også inn som sponsor for Amandusfestivalens manuskonkurranse, noe som resulterte i nok en kortfilm. Til sammen er det dermed produsert 12 filmer om personvern knyttet til «Du bestemmer». Alle disse filmene ble høsten 2008 distribuert til alle landets ungdomsskoler, sammen med et nytt hefte med tilvalgsstoff og oppgaver knyttet til filmene. Alle filmene er tekstet på bokmål, nynorsk, engelsk og nordsamisk.

Filmprosjektet ble nominert til PR-byråenes egen bransjepris «Gullkorn» i klassen for Årets holdningskampanje. «Du bestemmer» har tidligere også fått en internasjonal personvernpris («First special mention»).

Satsing mot mellomtrinnet

Inspirert av erfaringene med «Du bestemmer» rettet mot ungdom, har samarbeidspartnerne Utdanningsdirektoratet, Teknologirådet og Datatilsynet utvidet samarbeidet til også å utvikle et undervisningsopplegg for elever i 5-7. klasse. Bakgrunnen for dette er at mange har etterspurt et lignende opplegg mot de noe yngre elevene. Den nye skolepakken vil være ferdig i løpet av første halvår 2009. Dette materiellet vil naturlig nok ha en noe annen tilnærming, og berøre temaer som er særlig relevant for aldersgruppen, blant annet digital mobbing.

Internasjonal oppmerksomhet

«Du bestemmer» har vært gjenstand for stor internasjonal oppmerksomhet. Undervisningsopplegget er blitt presentert på flere internasjonale møter og konferanser. Mange land har allerede

benyttet hele eller deler av materialet slik det foreligger, oversatt til eget språk. Spania har lansert undervisningsopplegget på spansk og baskisk. Også Makedonia og Slovenia har tatt i bruk materialet fra Norge. Det har i tillegg kommet henvendelser fra Tyskland, Sveits, Danmark og Isle of Man med tanke på kunne benytte dette. Kanadiske personvernmyndigheter har for sin del etablert en filmkonkurranse for ungdom, i følge dem selv etter inspirasjon fra «Du bestemmer».

Bilder av barn på Internett

I oktober ble en veileder om bilder av barn på Internett distribuert til alle landets barnehager, samt skoler med 1 -7 trinn. Dette førte til en rekke etterbestillinger, og tilbakemeldingene har vært overveldende positive. Informasjonsbehovet har åpenbart vært stort. Veilederen har blitt brukt som grunnlag for diskusjon både på personal- og foreldremøter, og bevisstheten i skoler og barnehager om deres publisering av bilder av barn ser ut til å ha økt. Allerede i desember gikk første opplag av brosjyren (40 000 eksemplarer) tomt, og nytt måtte trykkes.

Brosjyren ble lastet ned 5 528 ganger fra Datatilsynets hjemmeside.

Veilederen er bygd opp rundt intervju med personer som har ulike innfallsvinkler til nettpublisering; Barneombudet, en etterforsker i Kripos, en pedagog, en forelder og en ungdom. Hvert intervju avsluttes med noen tommelfingerregler og diskusjonsoppgaver. Det er også med en del konkret fakta, for eksempel om lovverket og barnekonvensjonens bestemmelser.

Personvern i kunsten

Sommeren 2007 bevilget Fornyings- og administrasjonsdepartementet ekstra midler til et prosjektet hvor personvern skulle uttrykkes gjennom kunst. Datatilsynet ønsket å skape debatt og refleksjon rundt personvern gjennom å involvere kunstneriske uttrykk. Tilsynets hovedstrategi for å nå dette målet var å oppnå bred pressedekning og oppmerksomhet både i forkant av og under selve utstillingsperioden. For å sikre den kunstfaglige kompetansen ble det inngått en avtale med KORO (Kunst i offentlige rom, tidligere Statens utsmykningsfond). Når det gjelder utstillingslokaler ble det inngått samarbeid med Rom for kunst på Oslo S (ved Kulturbyrået Mesèn). I februar ble det utlyst en idékonkurranse med tittelen «Privatlivets fred». Innleveringsfrist, juryering og kåring av fire vinnere foregikk i april. Utstillingen «Privatlivets fred» ble åpnet av statsråd Heidi Grande Røys midt i ankomsthallen på Oslo S den 1. oktober. Der stod den til 26. november.

Dette har vært et utradisjonelt prosjekt for Datatilsynet og det var derfor vanskelig å forutse mottagelsen blant publikum og presse. Utstillingen med de fire kunstverkene oppnådde stor pressedekning, til sammen 43 oppslag i hele perioden fordelt på aviser, magasiner, radio og tv. I utstillingsperioden stod Datatilsynet også på stand på Oslo S. Dette viste seg å være en fin måte for Datatilsynet å gjøre seg synlig og tilgjengelig for publikum, samt å få tilgjengeliggjort tilsynets informasjonsmateriell.

Personvernrapporten

«Personvernrapporten 2008 – hva er vi redde for?» handler om hva som skjer i pressituasjoner der den grunnleggende muligheten til personvern blir svært vanskelig – eller umulig. Datatilsynet ser at det ofte er i bekjempelsen av det vi frykter mest, som kriminalitet, terror, helsesvikt og så videre, at de mest inngripende forslagene kommer. Under slike omstendigheter godtar vi kanskje lettere at de berørte blir fratatt selv den siste lille rest av personvern. Rapporten inneholder også funn fra en fersk personvernundersøkelse, artikler om personvern og offentlighet, id-tyveri og datalagringsdirektivet.

Personvernrapporten ble lansert i april med en pressefrokost, som resulterte i solid medieomtale og påfølgende bestillinger. Den ble også førstegangsdistribuert til over seks tusen mottakere. Ved årsskiftet var det kommet inn 463 etterbestillinger av til sammen 1782 eksemplarer. Rapporten har i tillegg blitt lastet ned mer enn 7200 ganger fra Datatilsynets hjemmeside.

Utstilling om ID-tyveri

Datatilsynet deltok i løpet av meldingsåret i utviklingen av en såkalt «hot-spot»-utstilling om ID-tyveri. Georg Apenes forestod åpningen av utstillingen, som stod på Teknisk Museum fra medio juni til medio september. Målet med utstillingen var å bidra til å styrke bevisstheten om identitetstyveri. Den viste, blant annet gjennom interaktive installasjoner, hvordan kriminelle får tak i våre personopplysninger, hvordan disse kan misbrukes og hvordan vi kan beskytte oss mot tyveriene. Andre bidragsytere var Kripos, Teknologirådet, NorSIS og Security Valley. Datatilsynet mener denne ut-

stillingen på en fin og lettfattelig måte demonstrerer hva begrepet ID-tyveri innebærer, og hvorfor det er relevant for alle som i en eller annen sammenheng oppgir sine personopplysninger. Datatilsynet har derfor tatt initiativ til å få videreført utstillingen på vitensentre andre steder i landet.

Datatilsynets hjemmeside

Hjemmesiden www.datatilsynet.no er en viktig kanal for Datatilsynet. Det legges stor vekt på å bruke nettsiden aktivt. I 2008 ble det publisert 80 egenproduserte nyhetssaker. I tillegg har Datatilsynet fortsatt den planmessige oppbyggingen og gjennomgangen av informasjonen om sektorer og teknologier.

Når forsiden oppdateres, sender Datatilsynet varsel til 3 322 abonnenter som selv har meldt seg på varslingslisten. Nytt i meldingsåret er at Datatilsynet, i tillegg til nyhetsvarselet per epost, også har gjort det mulig for leserne å melde seg på en rss-tjeneste. Her vil abonnenter få tilgang til nye saker i det øyeblikket de blir publisert. Det ser ut til at denne tjenesten er blitt vel mottatt. Bare i desember 2008 hadde Datatilsynet over 16 000 treff på denne tjenesten.

Mediekontakt

2008 har vært et aktivt år også når det gjelder arbeidet opp mot mediene. Dette skyldes blant annet den store oppmerksomheten omkring temaer som datalagringsdirektivet og identitetstyveri.

I løpet av 2008 har Datatilsynet registrert hele 1 614 henvendelser fra mediene, formidlet via Informasjonsavdelingen. Det ble i de aller fleste tilfellene gitt intervjuer og kommentarer til aviser, tv, radio eller internettbaserte medier. Dette har resultert i over seks tusen registrerte medieoppslag hvor Datatilsynet er omtalt.

Noen saker som fikk særlig stor medieomtale i 2008 er:

- Datalagringsdirektivet
- Den svenske FRA-loven
- Identitetstyveri
- Skattedirektoratets lekkasje av personopplysninger
- Kunnskapsdepartementets forslag om elevregister
- Elevundersøkelse stoppet av Datatilsynet
- Kameraovervåking på skoler og badeanlegg
- Nasjonalbibliotekets lagring av blogger mv

Tabell 1.1

	2005	2006	2007	2008
Antall foredrag	92	157	140	162

Datatilsynet har i meldingsåret også utarbeidet flere egenproduserte artikler og debattinnlegg enn tidligere.

Foredragsvirksomhet

Datatilsynet tilbyr normalt ikke egne seminarer eller kurs ut over de som arrangeres i forbindelse med personvernombudsordningen. Så langt tilsynet har tilgjengelige ressurser stiller vi imidlertid med foredragsholder på kurs og seminarer i regi av andre. Datatilsynets inntrykk er at våre foredrag/foredragsholdere er populære, da vi året igjennom mottar en jevnt høy strøm av forespørsler om foredragsholdere. I 2008 har vi holdt flere foredrag enn noen gang tidligere. Dette skyldes i stor grad oppmerksomheten omkring temaene datalagringsdirektivet og id-tyverier. I tillegg til foredrag i regi av andre har vi også hatt fire klassebesøk i 2008. Vi tok også initiativet til et seminar om kameraovervåking, holdt i samarbeid med Næringsforeningen i Trondheim og Samarbeidsgruppen Midtby'n.

Publikumsveiledning

Datatilsynet legger stor vekt på å være til stede og yte god bistand overfor de enkeltpersoner og representanter for virksomheter som på eget initiativ tar kontakt for å søke råd og veiledning. De aller fleste direkte publikumshenvendelser blir derfor besvart av en juridisk svartjeneste, som trekker på teknologisk kompetanse når det er nødvendig.

Den juridiske svartjenesten har i 2008 registrert 7 070 besvarte telefonhenvendelser, mot tilsvarende 7 300 året før. Dette utgjør en marginal nedgang. Imidlertid er det en oppgang i antallet henvendelser per e-post. Sett samlet har dermed antallet mer uformelle henvendelser per telefon og e-post gått noe opp i forhold til året før. Tilgjengelighet/svartid på telefonservicen vurderes gjennomgående å være meget god.

Hva handler henvendelsene om?

Tabellen nedenfor viser telefonhenvendelsene besvart av den juridiske svartjenesten. Henvendel-

Tabell 1.2

2008	Sum Plikt	Sum Rett	Total	Prosent
Annet	384	897	1281	18 %
Arbeidsliv	584	498	1084	15 %
Barn/Ungdom	108	61	169	2 %
Biometri	14	16	30	0 %
Fødselsnummer	80	773	853	12 %
Helse/Forskning	188	94	282	4 %
Informasjonssikkerhet besvart FS	146	64	210	3 %
Internasjonalt (overføring utland)	85	28	113	2 %
Internett (over 18 år)	154	291	445	6 %
Kameraovervåking	342	245	587	8 %
Kunderegister/medlemsregister	209	95	304	4 %
Melding/konsesjon	586	54	640	9 %
Reservasjon – DM	66	433	499	7 %
Velferd	38	53	91	1 %
Økonomi	147	335	482	7 %
Sum	3133	3937	7070	100 %

sene er fordelt på tema, og hvorvidt innringer opptrer som (eller på vegne av) plikt- eller rettighetshavere.

Tilsyns- og sikkerhetsavdelingen besvarte om lag 1000 henvendelser om informasjonssikkerhet.

Arbeidsliv er fortsatt det temaet det kommer flest henvendelser om, selv om det har vært en nedgang fra året før. Hele 15 prosent av henvendelsene gjelder dermed spørsmål knyttet til innsyn i e-post samt kameraovervåking og annen overvåking i arbeidslivet. I tillegg er en del av de henvendelser som er kategorisert som «biometri» relatert til arbeidslivet. Det har vært en relativt stor prosentvis økning i henvendelser knyttet til bruk av fødselsnummer sammenlignet med fjorårets tall (ni prosent). Dette kan trolig knyttes til at Datatilsynet har hatt et økt fokus på fødselsnummer som kilde til identitetstyveri. Temaet har også vært mye omtalt i mediene.

Tabell 1.3

År	2004	2005	2006	2007	2008
Antall tlf.henvendelser om DM	1 496	838	617	505	433

Utvikling i antall henvendelser om direkte markedsføring fra rettighetshavere

Nedgangen i antallet henvendelser om direkte markedsføring, særlig knyttet til reservasjonsregisteret, fortsetter. Datatilsynet mottok 433 telefonhenvendelser fra rettighetshavere i 2008. Dette er en betydelig nedgang, særlig sett opp mot nær 1 500 henvendelser fire år tidligere.

Henvendelser pr e-post

Det har kommet inn 3 054 henvendelser per e-post til den juridiske svartjenesten, mot 2 673 året før.

Henvendelsene fordeler seg tematisk omtrent som ved telefonhenvendelser, dog slik at spørsmål vedrørende Internett og fødselsnummer utgjør en noe større andel av e-posthenvendelsene enn pr. telefon. Dette er helt på linje med resultatene fra 2007.

Den juridiske svartjenesten har nå gode rutiner mht besvarelse av e-post, slik at målsettingen om at gjennomsnittlig svartid på e-post ikke skal overstige to virkedager oppfylles. Ved årsskiftet var det ingen ubesvarte e-posthenvendelser.

Tilsyns- og sikkerhetsavdelingen besvarte i overkant av 500 e-posthenvendelser.

Veiledningsmøter om informasjonssikkerhet

Datatilsynet gjennomførte i underkant av 70 veiledningsmøter hvor innholdet primært var av teknisk art. Problemstillingene som ble drøftet var hvordan behandlingsansvarlig kan oppnå tilfredstillende beskyttelse av personopplysninger. Datatilsynet gir råd i forhold til konkrete problemstillinger og veileder virksomheten i forhold til hva de bør settes fokus på i informasjonssikkerhetsarbeidet. Ofte deltar også leverandører eller konsulenter til behandlingsansvarlig. Datatilsynet ser slike møter som et viktig bidrag til å oppfylle veiledningsplikten etter forvaltningsloven. Tilbudet blir godt mottatt av virksomhetene

7 Tilsyns- og sikkerhetsarbeid

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

Grunnlaget for tilsynsarbeidet ligger i dokumentet «*Strategi og metodikk for operativt tilsyn med personopplysningsloven*». Personopplysningslovens regler om internkontroll er basis for kontrollmetodikken. Dette innebærer vektlegging av systemrevisjon av dokumentasjon kombinert med verifikasjon av praksis. Videre legger virksomhetsplanen føringer for valg av sektorer, bransjer og tema. I tillegg gir tips og klager fra publikum viktige innspill.

Det overordnede målet med Datatilsynets tilsynsvirksomhet er i henhold til personopplysningsloven å bidra til etterlevelse av lovregler om behandling av personopplysninger. Det følger av personopplysningsloven § 42 at Datatilsynet blant annet skal kontrollere at lover og forskrifter som gjelder for behandling av personopplysninger overholdes.

Målet med operative tilsyn er:

- Å skaffe god kunnskap om trusler mot personvernet innen ulike typer bransjer.
- Å bruke erfaringer fra operativt tilsyn til å sette fokus på personvern i ulike sektorer og bransjer.
- Å identifisere grupper som er spesielt utsatt for krenkelser av personvernet.
- Å overvåke den teknologiske utviklingen og hvilke trusler dette medfører for den enkelte.
- Å sørge for at avvik fra regelverket hos en behandlingsansvarlig rettes opp.
- Å la erfaringer fra operativt tilsyn tilflyte publikum.

7.1 Generelt om kontrollene i 2008

I 2008 ble det gjennomført 141 kontroller mot et bredt spekter av virksomheter. Basert på føringer fra virksomhetsplanen, ble det fokusert på elektronisk kommunikasjon og Internett. Tematikken er ikke avgrenset til de primære aktørene innen telekommunikasjon, men omfatter også profesjonelle brukere av slik teknologi.

Nærmere omtale av tilsynene er tatt inn under den sektorvise gjennomgangen i fagdelen, del II. Imidlertid er noen generelle hovedtrekk nevnt under.

Datatilsynet konstaterer omfattende brudd på regelverket, i den forstand at tilsynet varslet eller fattet vedtak mot noe mer enn halvparten av virksomhetene som ble underlagt kontroll. De vanligste avvikene var brudd på krav om tilfredstillende informasjonssikkerhet og internkontroll.

Den høye andelen som får varsel om vedtak rettet mot seg, må leses i lys av at Datatilsynet driver risikobasert kontrollvirksomhet. Det innebærer at tallet antakelig ikke er representativt for alle virksomheter i landet.

Mørketallsundersøkelsen fra Næringslivets Sikkerhetsråd (NSR) i 2008 viser at hele 80 % av virksomhetene oppgir at de kjenner personvernregelverket, mens bare 50 % oppgir at de etterlever regelverket. Datatilsynet erfarer at personopplysningsloven begynner å bli bedre kjent blant virksomhetene enn før. Det skyldes trolig en kombinasjon av at lovverket nå er nærmere ni år gammelt og at tilsynets funn i ulike bransjer ofte er omtale i media.

Datatilsynet observerer at en del virksomheter, på tross av sin kjennskap til regelverket, ikke gjennomfører de aktiviteter regelverket forutsetter. Et såpass grunnleggende forhold som å skaffe en oversikt over hvilke personopplysninger som faktisk behandles i virksomheten, er en av manglene Datatilsynet ofte avdekker. Uten denne kunnskapen har virksomheten dårlige muligheter til å avklare hvilke plikter den har.

Kjennskap til regelverket er utgangspunktet for etterlevelse. Før virksomheten kan sies å ha implementert regelverket, må de imidlertid arbeide aktivt med personopplysningsvern internt. Datatilsynets kontrollvirksomhet viser at eksemplene på motkrefter er mange: Å følge personvernre-

gelverket tar tid og fokus bort fra kjerneoppgaver, krever kanskje vesentlige investeringer, gir lite direkte bidrag til bunnlinjen, og kan kreve vesentlig tid fra ressurspersoner i organisasjonen. Selv om det å følge personvernregelverket kan gi langsiktige, positive effekter, ser det ut til at mange virksomheter velger å ikke investere tid og penger for å oppnå den gevinsten. Dette gjelder særlig dersom risikoen forbundet med at det blir oppdaget at virksomheten bryter regelverket er liten. I den grad en virksomhet blir oppdaget, hevder mange at regelverket er vanskelig tilgjengelig. Tilsynsmyndigheten ser likevel at en del av de behandlingsansvarlige som hevder dette, ikke har gjort reelle forsøk på å sette seg inn i hvilke plikter de har. I mange tilfeller har virksomheten verken sett på regelverket, eller oppsøkt kilder for veiledning, som for eksempel Datatilsynets hjemmeside.

Veileder om databehandleravtaler

Gjennom flere tilsyn har Datatilsynet avdekket uryddige tilstander i forholdet mellom behandlingsansvarlig og databehandler. I denne type forhold er det ofte databehandleren som sitter med alle kortene på hånden. Slik skal det ikke være. Databehandleravtalen skal skape likevekt i forholdet.

I mange tilfeller eksisterer det ingen databehandleravtale. I andre tilfeller mener man at andre avtaler mellom partene regulerer dette godt nok. Selv der man har laget en databehandleravtale er det ofte betydelige mangler ved den.

Databehandleravtalen kan gjerne inngå som et eget kapittel i egne tjenesteavtaler (driftsavtaler) mellom partene. Avtalen må imidlertid inneholde et minimum av bestemmelser som ivaretar de registrertes rettigheter etter personopplysningsloven. All bruk av personopplysninger mellom start- og sluttidspunkt må reguleres i avtalen. Datatilsynet mener avtalen ikke uten videre kan standardiseres, og har som en konsekvens av dette laget et informasjonsskriv om hva databehandleravtalen som et minimum må inneholde.

7.2 Personopplysninger på avveier i 2008

Personopplysningsforskriften pålegger behandlingsansvarlige å melde fra til Datatilsynet dersom personopplysninger som skal behandles konfidensielt kommer på avveier. Datatilsynet har merket en økning i antall pliktmessige meldinger om sikkerhetsbrudd i virksomhetene. Det kan være et uttrykk for større bevissthet rundt håndtering av avvik.

Fra 2008 vil Datatilsynet trekke frem Skatteetatens uautoriserte utlevering av fødselsnumre ved utsendelse av cd-er med skattelister til en del medier som den viktigste enkelthendelsen. Denne hendelsen rammet i praksis hele den voksne befolkningen. Datatilsynet vil også trekke frem et par enkelthendelser fra helsesektoren, henholdsvis tap av en minnepenn med flere journaler fra PPT-tjenesten, samt en sak der medisinske papirjournaler ble gjenglemt i en butikk etter endt handel. I meldingsåret ble det også mottatt melding fra et politisk parti om en mulig lekkasje av medlemslister.

I tillegg registrerte Datatilsynet flere hendelser der personopplysninger utilsiktet ble publisert i offentlige postlister, samt utlevert ved elektronisk dokumentinnsyn. De vanligste avvikene i slike saker er at en kommune utilsiktet publiserer private opplysninger om ansatte eller innbyggere på Internett.

Datatilsynet tror det er en betydelig underrapportering fra virksomhetene. Uten at dette kan kvantifiseres fornemmer tilsynet at mange virksomheter ikke melder avvik før det er fare for, eller er konstatert, at hendelsen likevel vil bli allment kjent. Et eksempel på dette fra meldingsåret er et helseforetak som først sendte avviksmelding for et alvorlig avvik til Datatilsynet etter at den berørte pasienten insisterte på det.

Det kan likevel se ut til at når virksomheter først begynner å melde avvik, senkes terskelen for å gjøre dette ved neste anledning.

Virksomheter har ikke formell plikt til å varsle berørte personer når personopplysninger kommer på avveier. Mange virksomheter velger å «dysse ned» saken overfor sine kunder eller brukere. Manglende kunnskap kan gi alvorlige konsekvenser for den enkelte. Det forhindrer den registrerte fra å utøve sine rettigheter, søke erstatning, eller å ta sine forholdsregler. Dersom det skal innføres en plikt til å varsle de berørte, kreves det justeringer i personopplysningslovens bestemmelser om informasjonsplikt.

Ny veileder: «Når ulykken er ute»

Datatilsynet har utarbeidet en veileder med tittelen «Når ulykken er ute». Denne gir virksomhetene konkrete råd når personopplysninger er på avveier eller står i fare for å komme på avveier. Veilederen er også integrert i bransjenormen for helsesektoren.

7.3 Nøkkeltall

Datatilsynets kontrollvirksomhet i 2008 omfatter kontrollaktiviteter mot i alt 141 virksomheter.

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

Tabell 1.4

Bransje/Sektor	Antall
Advokater	4
Arbeidsliv	1
Biometri	3
Databehandler – elektronisk kommunikasjon	2
Elektronisk kommunikasjon	10
Finanssektor – kredittkort	3
Kameraovervåking	41
Forsikring	1
Forskning	1
Forsvaret	2
Helse	11
Identitetsforvaltning – identitetskort	1
Innkreving	2
Justissektoren	6
E- forvaltning – kommune	11
Kredittopplysning	5
Krisesentre	5
Kundeopplysninger	1
Nummeropplysning	1
Personprofiler / personlighetstester	3
Samferdsel – flåtestyring	2
Staten	3
Utenrikstjenesten	3
Utdanning – læringsplattformer	7
Utlendingsforvaltningen	7
Varsling	5
Sum	141

Av de 141 kontrollene var 139 stedlige kontroller. Alle kontrollobjekter fremgår av vedlegg I.

DEL II

8 Temaer og tendenser i 2008

En viktig del av Datatilsynets mandat er å identifisere farer for personvernet, og gi råd om hvordan de kan unngås eller begrenses. Datatilsynet vil trekke frem sju tendenser som har vært særlig fremtredende i meldingsåret.

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

8.1 Ansvarsfraskrivelser svekker personvernet

Datatilsynet vil påpeke tre forhold som svekker, eller i verste fall pulveriserer, de rettighetene vi som individer har etter personvernregelverket.

1) Uklare ansvarsforhold

Personopplysningsloven legger ansvaret for behandlingen av personopplysninger til en behandlingsansvarlig. Bakgrunnen for ansvarsplasseringen er at en definert instans skal ha ansvaret for at personvernet blir ivaretatt, både forholdet til borgernes rettigheter, og myndighetenes krav.

Tilsynene i 2008 viser uklare ansvarsforhold for mange databaser og registre med personopplysninger. I noen sammenhenger har uklarhetene utspring i en komplisert organisering av en virksomhet, som for eksempel i konsernstrukturer eller i arbeidsfellesskaper mellom privatpraktiserende leger eller advokater.

Det finnes imidlertid også uklare ansvarsforhold for databaser de fleste ville tro har en trygg forankring i en etat eller et forvaltningsorgan. Datatilsynet så i meldingsåret på to støttesystemer for kostnadsfordeling opprettet i Helse Sør-Øst RHF. Datatilsynet mente at det regionale helseforetaket instruerte sine underliggende helseforetak til å gå inn i ulovlig praksis ved å koble seg til disse to systemene. Systemene var bestemt og fastlagt av det regionale helseforetaket, mens de underliggende helseforetakene ble utpekt som behandlingsansvarlig. De sistnevnte hadde imidlertid ikke reelle muligheter til å ivareta sine plikter

etter personopplysningsloven. Les mer om dette i avsnittet om helse og forskning.

Kontroller i 2008 viste at plikten til å informere berørte parter om politiets fingeravtrykksregister AFIS ikke ble etterlevd. Fingeravtrykkene blir lagret i AFIS samtidig med at de blir lagt inn i EURODAC, et strengt regulert europeisk fingeravtrykksregister. Der opplysninger i AFIS kan brukes i etterforskning, vil opplysninger i EURODAC ikke være tillatt brukt til dette formålet. Resultatet av manglende informasjon er dermed at asylsøkerne ikke får vite at fingeravtrykkene de har avgitt kan bli brukt i etterforskning. Utlendingsloven fastslår at Kripos er registeransvarlig, og Justisdepartementet er registereier for AFIS. Kripos problematiserte imidlertid ansvarsfastsettelsen. Saken er ikke avklart når årsmeldingen skrives. Les mer i kapittelet om justissektoren, avsnittet om utlendingsfeltet.

Forslaget til ny folkeregisterlov, fremlagt i meldingsåret, legger opp til at det nye folkeregisteret skal være et slags «dugnadsprosjekt» der ansvaret for at personopplysningene er korrekte, oppdaterte og tilstrekkelige er tenkt lagt til flere aktører med tilgang til registeret. Datatilsynet var i sin høringsuttalelse bekymret for at ansvaret blir pulverisert når det ikke er tydelig plassert.

Eksemplene nevnt ovenfor er typiske uklarheter som kan gi store personvernkonsekvenser for den enkelte.

Datatilsynet understreker at det er spesielt viktig at den som lager datasystemer der flere instanser skal bidra med, eller bruke, personopplysninger, også plasserer ansvaret tydelig, samt ser til at ansvarshaveren har midler og reell myndighet til å følge opp sine plikter.

2) Uryddige databehandleravtaler

Noen virksomheter velger å sette ut hele eller deler av behandlingen av personopplysninger til andre virksomheter, såkalte databehandlere. Valget kan skyldes at virksomheten mangler kompetanse til å forestå driften selv, eller at virksomheten vurderer det som hensiktsmessig eller lønnsomt av andre årsaker. Ofte vil databehandlere ha spesialkompetanse innen «sine» tjenesteområder. Selv om den behandlingsansvarlige virksomheten bruker databehandlere, har den fortsatt ansvaret for å sikre, gjennom avtaler og oppfølging, at personopplysninger behandles i tråd med regelverket, og at sikkerheten er tilstrekkelig.

Funn under kontrollvirksomheten viser at mange av virksomhetene som bruker databehandlere, ikke har etablert tilstrekkelige avtaler, slik personopplysningslovens § 15 krever. Konsekvensen er at den enkelte registrerte får et betydelig dårligere rettsvern enn han eller hun skulle hatt etter personopplysningsloven.

Regelverket forutsetter at det er den behandlingsansvarlige som skal sette premissene. Tilsynene i 2008 viser imidlertid at dette ofte ikke er tilfellet. Den behandlingsansvarliges muligheter til å disiplinere databehandlere oppleves i mange tilfeller som begrenset. Den behandlingsansvarlige oppfatter at den enten må akseptere standardavtalen til databehandleren, eller finne seg en annen leverandør.

3) Manglende systematisk internkontroll

Internkontroll er den behandlingsansvarliges virkemiddel for å sikre at virksomheten opererer i samsvar med regelverket. Fravær av et slikt system overlater etterlevelsen av regelverket i for stor grad til tilfeldighetene. Mer enn halvparten av kontrollerte virksomheter får anmerkninger om manglende eller utilstrekkelig internkontroll. Ofte har virksomheten ikke laget sentrale rutiner. I noen tilfeller har Datatilsynet observert at det ikke har vært arbeidet med ivaretakelse av internkontrollplikten i det hele tatt.

8.2 Manglende sletting og gjenbruk til nye formål gir personvernkonsekvenser

Datatilsynet har i 2008 funnet systematiske brudd på regelverkets krav om sletting i alt for mange saker. Informasjonen beholdes i mange tilfeller på ubestemt tid og slettes kun når praktiske hensyn tilsier det. Lagring av data har blitt billigere og billigere, mens sletting av opplysninger krever en aktiv holdning til hvilke opplysninger man trenger, og hvilke man kan unnvære. I sum er det antakelig dyrere å etterleve tilstrekkelige sletterutiner enn å lagre opplysningene videre.

Datatilsynet kan konstatere at disse argumentene blir brukt til å forsvare videre lagring:

- Oppbevaring er nødvendig for å ivareta kundens beste, for eksempel i tilknytning til eventuelle klager. Argumentet svekkes imidlertid ofte ved at virksomheten unnlater å informere kunden om at opplysningene oppbevares på ubestemt tid.
- Oppbevaring er nødvendig av hensyn til annen lovgivning, som regnskapslovgivningen eller arkivlovgivningen. Denne lovgivningen krever

noe lagring, men antakelig ikke på et såpass detaljert nivå som det praksis ofte viser.

Det ser også ut til at flere aktører hevder at de gjerne vil oppbevare opplysningene videre, fordi de kan komme til nytte på et senere tidspunkt. Fra et personvernståsted er en slik utvikling dramatisk. I kjernen av personvernregelverket ligger et prinsipp om at opplysninger kun skal brukes til de formålene de ble innsamlet for, og at den registrerte skal få informasjon om bruken og formålet. Dermed kan den registrerte innrette seg etter de spillereglene som er presentert for vedkommende. Når opplysningene har oppfylt sitt formål, skal de slettes. Dette prinsippet blir brutt dersom personopplysninger lagres når de ikke lenger er nødvendige, eller når opplysningene blir brukt til nye formål. De registrerte har ingen mulighet til å kunne sette seg inn i alle nye bruksområder for opplysningene, og dermed har de heller ingen mulighet til å bruke sine rettigheter etter personopplysningsloven.

Datatilsynet har fått flere håndfaste eksempler på at personer, ved rene tilfeldigheter, har blitt konfrontert med opplysninger som skulle ha vært slettet. I en slik sak avgjorde Datatilsynet, og senere Personvernnemnda, at opplysninger om en 16 år gammel varetektsfengsling skulle vært slettet fra Det sentrale straffe- og politiopplysningsregisteret (SSP). Dette kan man lese mer om i kapittelet om justissektoren.

8.3 Anonyme alternativer forsvinner – og identifisering kreves, selv når det ikke er nødvendig

Datatilsynet har gjennom flere årsmeldinger påpekt tendensen til at de anonyme alternativene er under nedbygging eller avvikling. Dette gir et dårligere personvern i Norge. Spesielt har Datatilsynet inntrykk av at man, i det øyeblikket man går fra papirbaserte eller manuelle systemer til elektroniske systemer, gjerne tar i bruk de muligheter til detaljert registrering som fins i tilbudte løsninger. Lagring av detaljerte opplysninger om enkeltmenneskers bevegelser eller bagatellmessige kjøp blir spesielt betenkelig når man vet at opplysninger i etterkant sjelden blir slettet, som påpekt tidligere i dette kapittelet.

Kontanter og ikke-personlige klippekort er eksempler på anonyme alternativer. Kontantbetaling medfører at det ikke registreres opplysninger om pengebruk knyttet til person. Et forhåndsbetalt, ikke-personlige klippekort til bussen gjør at det ikke lagres opplysninger om hvem som foretok en bestemt reise på et gitt tidspunkt.

I meldingsåret saksbehandlet Datatilsynet flere saker der kollektivselskaper ønsker å bruke løsninger som er konstruert slik at den som reiser eller betaler, også identifiserer seg i det han eller hun bruker tjenesten. Identifiseringen kan finne sted ved at man må presentere et personlig kort, som ved elektroniske billetter, eller ved at en elektronisk brikke blir avlest automatisk, for eksempel ved avlesing av autopassbrikker i en bomring. Det ble i meldingsåret opprettet flere bomstasjoner som bruker autopassbrikken, en rfid-brikke med unik ID som etter hvert vil sitte i de fleste norske biler. I tillegg finnes det konkrete planer for å åpne for at autopassbrikken kan brukes i andre sammenhenger enn ved bombetaling, som for eksempel for å kreve inn betaling i parkeringshus. Datatilsynet er bekymret for at en stor økning i antallet avlesningspunkter for autopassbrikker kan gi detaljerte opplysninger om enkeltmenneskers bevegelser.

I 2008 ble det også foreslått en lovendring som åpner for at spesielt forurensende kjøretøyer kan pålegges ekstra avgifter når de kjører inn i bestemte områder (lavutslippsoner). Betalingsordningen som anbefales i lovendringsforslaget, er maskinell avlesning av registreringsnumre eller autopassbrikker. I praksis innebærer forslaget en hjemmel for registrering og kontroll av samtlige biler.

Datatilsynet mener at det bør være mulig å være anonym når identifisering er unødvendig, og følger derfor utviklingen tett. Les mer i kapittelet om samferdselssektoren.

8.4 Økt utveksling av data mellom databaser gir svekket personvern

Utviklingen går i retning av at stadig flere instanser skal dele, eller ha tilgang til, personinformasjon hos andre etater eller instanser. Hensikten er ofte å effektivisere prosessene. I meldingsåret var dette spesielt fremtredende innen justissektoren og helsesektoren, i tillegg til i den foreslåtte nye folkeregisterloven.

Innen justissektoren pågår en planmessig videreutvikling av systemer slik at utveksling av data i større grad skal kunne foregå på databasenivå. Etter Datatilsynets mening stiller denne utviklingen store krav til lovreguleringen av politiregistrene, et lovverk som er anerkjent mangelfullt, også av Justisdepartementet selv. Datatilsynet er oppmerksom på at det har vært arbeidet med et

lovutkast i Justisdepartementet i meldingsåret. Tilsynet har gitt konkrete innspill til hvilke endringer det mener er nødvendig i den nye politiregisterloven, blant annet bedring i fundamentale garantier som tilstrekkelig sletting/sanering av opplysninger, tilgangsstyring og taushetsplikt.

Passmyndigheten er i Norge lagt til politiet. Som følge av EUs krav til pass, skal fingeravtrykk lagres i en brikke på passet, og brukes til å sjekke at bæreren er samme person som den som fikk utstedt passet. I forslaget til endringer av den norske passloven vil man imidlertid gå lenger enn dette, og lagre fingeravtrykkene i det sentrale passregisteret i tillegg. Kripos og utlendingsmyndighetene skal etter forslaget få tilgang til dette registeret, uten at tilgangen er tilstrekkelig begrunnet i høringsforslaget. Det vil i praksis si at det opprettes et fingeravtrykksregister over store deler av den norske befolkningen til bruk for politiet – uten at dette er problematisert eller utredet. Datatilsynet er kritisk til en slik utvikling. Les mer om Datatilsynets innspill til politiregisterloven og passloven i avsnittet om justissektoren.

Den foreslåtte folkeregisterloven legger opp til at én stor database skal betjene alle forvaltningens ulike behov for opplysninger om personer. Forslaget tar utgangspunkt i at forvaltningens ulike, lokalt tilpassede databaser skal avvikles. Datatilsynet mener en slik utvikling over tid vil medføre at man får én stor database med mye overskuddsinformasjon i forhold til hva de fleste forvaltningsledd faktisk har behov for. Mer informasjon om dette forslaget finner man i avsnittet om identitet og biometri.

I 2008 sendte Helse- og omsorgsdepartementet ut et høringsforslag om å tillate helseforetak tilgang til hverandres helsejournalsystemer. I høringsuttalelsen reagerer Datatilsynet på at departementet ikke tar hensyn til de alvorlige mangler ved informasjonssikkerheten som er avdekket ved flere av landets helseforetak. Manglene knytter seg både til dårlig tilgangsstyring til pasientjournalene og til dårlig kontroll av journalenes logger. Datatilsynet er av den oppfatning at helseforetakene i det minste må få på plass tilfredsstillende tilgangsstyring internt før det bør bli aktuelt å åpne systemene for ekstern tilgang. Les mer om dette i avsnittet om helse og forskning.

8.5 Utilstrekkelig vern mot snoking

Datatilsynet har tidligere påpekt at mørketallene for urettmessig tilgang til personopplysninger internt i virksomheter trolig er store. Svært mange offentlige og private behandlingsansvarlige har mangelfull kontroll med hvem som slippes til i databasene. Derfor vil snokingen i mange tilfeller være vanskelig å avdekke.

Det har kanskje vært mest fokus på snoking i helsevesenet de siste årene. I forbindelse med at Justisdepartementet arbeider med ny politiregisterlov, finner Datatilsynet imidlertid at det er viktig å fremheve at dette også er et problem innen politi- og justissektoren. I politiregistrene Datatilsynet kontrollerte i meldingsåret ble ikke lesetilgang i databasene logget. Datatilsynet stilte også spørsmål ved om tilgangskontrollen var god nok, og om kriteriene for å bli autorisert som bruker var klare, tilgjengelige og dokumenterte. Les mer om disse kontrollene i avsnittet om justissektoren.

Virker det nye forbudet mot snoking i pasientjournal?

Selv om noen helseforetak har arbeidet systematisk for å forebygge snoking, viser det seg at de fleste har problemer med å etablere løsninger som sikrer at kun personer med tjenstlig behov får tilgang. Stortinget vedtok i meldingsåret et forbud mot snoking i pasientjournaler. I helseregisterlovens § 13a heter det at: «Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helseopplysninger som behandles etter denne loven uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift.» Brudd på bestemmelsen kan medføre bøter eller fengsel i inntil tre måneder.

Datatilsynet er opptatt av at man sikrer at dette forbudet får et reelt innhold. I meldingsåret hadde Helsetilsynet saker vedrørende snoking til behandling, uten at det har ført til reaksjoner. I ett tilfelle mente Helsetilsynet at det fantes en for stor mulighet for at andre enn passordinnehaveren hadde logget seg inn i pasientjournalen, og at identiteten til snokeren dermed ikke var tilstrekkelig dokumentert. Tilgangen til pasientjournalen var passordbeskyttet i tråd med dagens anbefalinger, men passordet ble oppbevart i nærheten av terminalen. Dette var i strid med interne retningslinjer ved helseforetaket. Datatilsynet frykter at forbudet mot snoking ikke vil virke etter sin hensikt dersom ikke kravene til sikkerhet også styrkes, slik at helseforetakene har reelle mulighet til å påvise hvem som har skaffet seg tilgang til hvilke opplysninger.

8.6 Uthuling av taushetsplikt

Datatilsynet er bekymret for at man, for å forenkle mulighetene for økt utveksling av personinformasjon mellom databaser, velger å uthule den lovbestemte taushetsplikten.

I meldingsåret ga Datatilsynet innspill til Justisdepartementet om behovet for gode taushetspliktsbestemmelser for politiet i forbindelse med arbeidet med politiregisterloven. I tilegg påpekte Datatilsynet til Helse- og omsorgsdepartementet at den foreslåtte tilgangen til helseopplysninger på tvers av helseforetak fører til en massiv uthuling av taushetsplikten helsepersonell i mellom. Ved tilgang til journalopplysninger skal man verken måtte hente inn samtykke fra pasienten, eller vurdere hvorvidt opplysningene er nødvendige og relevante for pasientbehandlingen. Dette vil medføre at helsepersonell får vid tilgang til overskuddsinformasjon, potensielt om hele landets befolkning.

Etterfølgende kontroll av logger i stedet for tilgangskontroll

Datatilsynet ser en tendens til at virksomheter velger å gi sine ansatte bred tilgang til databasene fremfor smal, oppgavebegrenset tilgang. I stedet for å begrense hvem som skal ha tilgang til hva, velger man eventuelt å logge oppslag i databasene.

Datatilsynet vil understreke at logging ikke kan erstatte tilgangskontroll ut fra personvernmessige betraktninger.

Virksomheter som argumenterer for at logging gir tilstrekkelig vern, mener ofte det vil være en altfor omfattende jobb å finne ut hvem som trenger tilgang til hva, og hvilke opplysninger virksomheten behandler. En slik oversikt er imidlertid et grunnleggende krav i personopplysningsloven.

Datatilsynet har tidligere påpekt at ansattes taushetsplikt blir brukt som argument for at den som har ansvar for å sikre opplysninger i et datasystem ikke innfører tilstrekkelig tilgangskontroll til opplysningene. Datatilsynet ser på dette som en ansvarsfraskrivelse på systemnivå, og er bekymret for at personvernet kun skal være opp til den enkelte ansattes integritet og egne vurderinger.

8.7 Stadig mer kameraovervåking til ulike formål

For bare ti til femten år siden så man kameraovervåking forholdsvis sjeldent, oftest ved ransutsatte virksomheter. Overvåkingen var i stor grad forbundet med tungtveiende sikkerhetsbehov, eller behov for å sikre fysiske verdier. Denne begrensningen er forlengst et tilbakelagt stadium. Flere aktører tar i bruk kameraovervåking til å ivareta andre behov og ønsker.

Saksbehandlingen, kontrollene og henvendelsene til Datatilsynet i 2008 viser at det er vanskelig å få øye på bransjer hvor kameraovervåking ikke benyttes. Man kan heller ikke konkludere med at en virksomhet har tatt i bruk kameraovervåking bare ved å se på hvilken type virksomhet det er. Det er like gjerne slik at kiosken har kameraovervåking, som at gullsmedbutikken har det.

Stadig flere formål blir trukket frem for å rettferdiggjøre kameraovervåking. Et eksempel fra en restaurant i Trondheim kan belyse denne observasjonen. Restaurantens hovedbegrunnelse for overvåkingen var muligheten for å kunne følge med på behovet for å rydde bord eller å betjene kundene. Overvåkingen gjorde at servitøren skulle få slippe å gå ut i serveringslokalet for å se etter. Datatilsynet har også fått henvendelser fra virksomheter som ønsker å bruke kameraovervåking for å se om det er kunder i lokalet slik at det er mulig å sitte på et bakrom, samt fra personer som ønsker å ha ubemannede løsninger av ulike slag.

Når terskelen for å igangsette kameraovervåking fjerner seg stadig mer fra de mest basale behov som sikkerhet og trygghet, blir grensedragningen en utfordring: Finnes det formål og begrunnelser som må anses som så svake at overvåking ikke lar seg rettferdiggjøre? Skal det finnes noen grense? Om man ikke er villig til å trekke denne grensen, er alternativet at kameraovervåking i prinsippet kan brukes til hva som helst, og kan finnes hvor som helst, så lenge personvernulempene, isolert, i hver enkelt, konkrete sak, er liten nok. I et større perspektiv er dette høyst betenkelig – ikke bare for personvernet. Les mer om dette i avsnittet om kameraovervåking.

Flere bruker falske overvåkingskameraer

Datatilsynet får stadig flere henvendelser fra personer som opplever sitt personvern krenket av overvåkingskameraer som ved nærmere ettersyn viser seg å være etterligninger, ikke ordentlige overvåkingskameraer. Bruk av slike dummy-kameraer reiser vanskelige, prinsipielle spørsmål.

Mange av sakene omhandler dummy-kameraer i nabolag og boligområder, men Datatilsynet ser også dummy-kameraer i bruk hos profesjonel-

le aktører, både utendørs og innendørs. I mange tilfeller er dummy-kameraene plassert slik at de ville representert en ulovlig overvåking dersom kameraene var ekte.

Selv om overvåkingen ikke er reell, vil følelsen av å være overvåket være ekte. I verste fall kan et ubrukelig plastikkamera gripe kraftig inn menneskers opplevelse av egen hverdag. Det være seg fordi man er forledet til å tro at naboen overvåker det man gjør hjemme, eller at arbeidsplassen er nærmest totalovervåket.

Datatilsynet oppfatter at mange tror at bruk av dummykameraer skåner den enkelte i høyere grad enn reell overvåking vil gjøre: Folk gis «bare» en følelse av å bli overvåket. Datatilsynet ser store problemer med en slik tilnærming. Det må stilles spørsmål ved om samfunnet er tjent med at borgernes handlinger blir forsøkt manipulert, eller for den saks skyld «forbedret», gjennom tilsynelatende overvåking.

Selv om det verken innsamles, lagres eller tilgjengeliggjøres personopplysninger, vil dummykameraer true sentrale personvernprinsipper. Ryddig og sannferdig informasjon er bærende elementer i personvernregelverket. Borgeren er avhengig av å kunne ha tillit hva han blir presentert for, det være seg informasjon i en samtykkeerklæring, informasjon på varselsskilter eller synlige overvåkingskameraer. Usannheter og tilbakeholdelse av informasjon svekker en viktig ressurs, nemlig tillit.

9 Nærmere om utvalgte saksfelter

9.1 Justissektoren

I justissektoren arbeides det nå på en rekke felter med økt utnyttelse av informasjon lagret i ulike databaser og registre. Dette gjelder både opplysningene i det norske politiets egne databaser, databaser hos private tele- og internettleverandører, samt databaser hos andre myndigheter, både innenlands og utenlands.

Tankegangen bak denne vide utnyttelsen er i direkte motstrid med tankegangen bak personvernregelverket, nemlig at opplysninger kun skal brukes til det formålet det er innhentet for. Dette ble blant annet påpekt i en rapport fra Europarådets *Kommisjonær for menneskerettigheter* i meldingsåret.

Funn under tilsynene ved enkelte av politiets registre, samt flere konkrete saker fra meldingsåret, har gjort at Datatilsynet ser med bekymring på personverntilstanden i politi- og justissektoren. Disse funnene og sakene er omtalt i avsnittene under. Bekymringen støttes også av funn under tilsynet ved Ila fengsel i 2007, samt andre utviklingstrekk omtalt i Datatilsynets årsmeldinger fra 2007 og 2005.

9.1.1 Politiets registre

Utilstrekkelig politiregisterregelverk

Det har lenge vært enighet om at det norske politiregisterregelverket er utilstrekkelig. I følge Justisdepartementet ble det i 2008 arbeidet med å ferdigstille et forslag til en ny lov for dette området. Arbeidet har blitt forsinket, blant annet har man avventet et EU-initiativ,

> «Rammebeslutning om beskyttelse av personopplysninger i forbindelse med politisamarbeid og rettslig samarbeid i kriminalsaker».

Denne EU-beslutningen ble ferdigstilt mot slutten av 2008, som et minimumsregelverk som ikke stiller store krav til nasjonal lovgivning. Datatilsynet er bekymret for at man, inspirert av dette rammeverket, vil velge en for svak beskyttelse av personopplysninger i politisektoren nasjonalt.

Datatilsynet har hatt fokus på justissektoren gjennom tilsyns-, hørings- og utvalgsarbeid gjennom flere år. Gjennom arbeidet har Datatilsynet understreket følgende:

- Det er behov for klare regler for sletting eller sanering av opplysninger hos politiet. Ved utvikling av politiets databaser har man hatt fokus på hvilke handlinger som skal kvalifisere for å bli registrert i politiets registre. Spørsmålet om når opplysninger skal ut av databasene har sjelden vært berørt. Problemstillingen kommer til å bli ytterligere aktualisert i årene fremover i tråd med den planmessige oppbyggingen av utveksling mellom databaser innenlands og utenlands, og bedre muligheter til samtidige søk i flere databaser.
- Det er behov for avklarte ansvarsforhold og ryddig rollefordeling for behandlingen av personopplysninger mellom aktører innen politisektoren, og innen tilstøtende organer der dette er aktuelt, for eksempel hos utlendingsmyndighetene.
- Det er behov for å etablere gode prinsipper for tilgangsstyring internt i politiet basert på at ansatte kun får tilgang til de opplysningene de har behov for i sitt arbeide.

– Datatilsynet ser at en regulering av politiets taushetsplikt bør være en del av arbeidet med en ny politiregisterlov.
– Datatilsynet etterlyser en bedre regulering av politiets tilgang til andre aktørers databaser.

I tillegg har Datatilsynet oppfordret politisektoren til å oppnevne et personvernombud.

Sletting i politiregister

Personvernnemnda har i 2008 tatt stilling til en slettesak i politiregisteret *Det sentrale straffe- og politiopplysningsregisteret* (SSP).

Saken gjaldt en person som ble stoppet ved en grensepassering i 1988, og varetektsfengslet etter mistanke om besittelse av hasj. Klageren ble holdt i varetekt i tre uker, og senere sluppet fri, uten at det ble reist tiltale i saken.

Klageren var ikke oppmerksom på at disse opplysningene fremdeles befant seg i politiets registre, før politiet konfronterte ham med den gamle saken 16 år senere, ved en annen grensepassering.

Personopplysningsloven gjelder ikke for saker som behandles i medhold av rettspleielovene, etter et unntak i personopplysningsforskriften. Datatilsynet mente imidlertid at personopplysningsloven kom til anvendelse på opplysningene i denne saken, fordi lovgiver ikke har tatt stilling til hvor lenge opplysninger i politiopplysningsdelen i SSP bør lagres. Derfor vil personopplysningsloven, etter Datatilsynets mening, gi utfyllende bestemmelser.

Kripos mente at opplysningene ikke ble omfattet av personopplysningsloven, og at Datatilsynet derfor ikke hadde kompetanse til å kreve sletting.

Personvernnemnda sa seg enig med Datatilsynet, og mente at personopplysningsloven kom til anvendelse. Personvernnemnda kommer frem til at det er en grense for hvor lenge man må tåle å stå registrert i et nasjonalt register: Inntil domstolen har fattet sin beslutning, vil opplysningene være unntatt bestemmelsene i personopplysningsloven. Etter at domstolen har sagt sitt, vil personopplysningsloven regulere videre bruk og tilgjengeliggjøring.

Saksgangen avdekket en svært vid tilgang til opplysningene i dette politiregisteret. Personvernnemnda påpeker spesielt at det er bekymringsfullt at over 13 000 tjenestemenn har full tilgang til opplysninger om varetektsfengsling og andre sensitive opplysninger. Tilgangen er gitt uten tidsbegrensning, og uten at det tjenestemessige behovet for tilgang ser ut til å være vurdert. Personvernnemnda oppfordrer politiet til å lage en mindre inngripende ordning.

Tilsyn hos politiet

Datatilsynet gjennomførte i 2008 flere kontroller hos Politidirektoratet (POD) og ved politidistriktene. Formålet med kontrollene var å vurdere om behandlinger av personopplysninger som ikke var direkte knyttet til tradisjonell politietterforskning skjedde i samsvar med personopplysningslovens bestemmelser.

Totalt ble det gjennomført seks kontroller i sektoren. Datatilsynet så nærmere på passregisteret, nasjonalt våpenregister og prikkbelastning av førerkort. I tillegg ble det gjennomført kontroll ved to politikamre knyttet til kameraovervåking i arrest, samt ved en personalbarnehage ved Oslo politikammer.

På kontrolltidspunktet var få av behandlingene av personopplysninger meldt til Datatilsynet i tråd med personopplysningslovens krav.

Internkontrollen var mangelfullt utarbeidet. Det var særlig styrende og kontrollerende elementer som fremstod som mangelfulle.

I tillegg ble følgende påpekt:

a) Våpenregisteret

Datatilsynet konkluderte med at våpenregisteret ikke ser ut til å tilfredsstille nødvendige krav til kvalitet (at opplysningene er korrekte, oppdaterte og ikke lagret lenger enn nødvendig). Det ble gitt pålegg om endring av rutinene for registrering og oppdatering av opplysninger.

Det store antallet registrerte døde personer og manglende oppdatering av registerets adresseopplysninger innebærer et usikkerhetselement ved registerets kvalitet.

Datatilsynet påpekte også at registeret mangler enhetlig struktur og standardisering.

Manglende etterkontroll av vilkårene for å kunne eie våpen innebærer et usikkerhetselement ved registerets kvalitet.

b) Prikkbelastningsregisteret

Datatilsynet konkluderte med at det må foretas en gjennomgang av rutinene for utlevering av personopplysningene i prikkbelastningssystemet til eksterne aktører, herunder sikre at kun nødvendig informasjon overføres og at overføring kun skjer til autorisert personell.

Opplysninger om prikkbelastninger skal slettes når de ikke lenger er nødvendige. Prikker som er ilagt for mer enn tre år siden skal slettes.

c) Billedopptak i politiarrestene

Det må etableres sletterutiner slik at billedopptak i politiarrestene ikke lagres lenger enn det som er nødvendig ut fra formålet med behandlingen. Datatilsynet viser til at Politidirektoratet, i et rundskriv, har uttrykt at lagring i mer enn 48 timer vanskelig vil kunne anses som nødvendig.

Fingeravtrykk i pass og i det sentrale passregisteret

I meldingsåret ble passloven foreslått endret slik at passmyndigheten skal få hjemmel til elektronisk lagring av fingeravtrykk, i tillegg til en rekke andre opplysninger, i det sentrale passregisteret.

Datatilsynet skrev i sin høringsuttalelse at de foreslåtte endringene i passloven åpner for unødvendig, udefinert og ukontrollert bruk av fingeravtrykk.

Tilsynets viktigste merknader til de foreslåtte endringene er:

- Datatilsynet er i mot opprettelse av et sentralt passregister med biometriske data som fingeravtrykk og signatur. Det sentrale passregisteret vil, om denne informasjonen inkluderes, inneholde tilstrekkelig informasjon til å produsere duplikater av pass, selv uten innehaverens aktive medvirkning.
- Datatilsynet er ikke i mot at biometrisk teknologi benyttes i selve passet for å kunne identifisere passinnehaveren. Imidlertid er Datatilsynet i mot at det skal lagres detaljrike bilder av fingeravtrykk i passene, samt i det sentrale passregisteret. Løsningen kan etter Datatilsynets oppfatning medføre fare for kompromittering av andre biometriske sikkerhetsløsninger ved at fingeravtrykksbilder med høy oppløsning kan være for lett tilgjengelige eller komme på avveier.
- Datatilsynet er bekymret for at en for vid gruppe personer skal kunne skaffe seg tilgang til informasjonen i passene og i det sentrale passregisteret.

Gjennom flere kontroller mot passmyndighetene har Datatilsynet avdekket utilfredstillende forvaltning av den eksisterende ordningen. – Bekymringen blir ikke mindre av de foreslåtte endringene, skrev Datatilsynet i høringsuttalelsen.

9.1.2 Politiets radiosamband er fortsatt tilgjengelig for alle

Utbygging av et landsdekkende, avlyttingssikkert samband for nødetatene har pågått i noen år. Datatilsynet erfarer stadig at sensitive personopplysninger lekker ut fra politiets nødsamband. Det er i tillegg etablert flere internettbaserte tjenester som videreformidler politidistrikters samband. Kommunikasjonen kan også enkelt legges inn på hvem som helst sin mobiltelefon. I praksis kan derfor enhver lytte til politiets kommunikasjon. Det er gått flere år siden Datatilsynet påla politiet og de andre nødetatene å sikre sine samband, og tilsynet er bekymret for de forsinkelser utbyggingen stadig har vært utsatt for. Ikke bare er dette en stor utfordring for det politioperative arbeidet ved at kriminelle kan lytte og disponere deretter, men Datatilsynet er også sterkt bekymret for at ofre, vitner eller andre som ringer politiet risikerer å få kringkastet sine personopplysninger.

Datatilsynet håper de nødvendige ressurser stilles til rådighet for raskest mulig å realisere målet om et landsomfattende nødnett.

9.1.3 Justissektoren internasjonalt

Videreutviklingen av Schengen informasjonssystem – SIS

Justisdepartementet foreslo i meldingsåret å gi tollmyndigheten direkte tilgang til Schengen Informasjonssystem (SIS), en database ment å avhjelpe ulempene ved å ha åpne grenser innen Schengen-området. Datatilsynet, som er det organ som skal kontrollere etterlevelsen av SIS-regelverket, er bekymret for at stadige utvidelser i antallet forvaltningsmyndigheter som gis direkte aksess, går på bekostning av personvernet til de mange hundre tusen registrerte i systemet.

De foreslåtte utvidelsene i spekteret av personopplysninger som skal registreres i neste generasjons informasjonssystem (SIS II), innebærer også at biometriske data, som fotografi og fingeravtrykk skal registreres i databasen. Tilsynet mener derfor at lovgiver bør være tilbakeholden med å utvide antallet forvaltningsmyndigheter med direkte tilgangsrettigheter. Et stort antall forvaltningsorganer med direkte tilgang kan dessuten vanskelig sies å være forenlig med SIS-loven § 1, som slår fast at ett av formålene med SIS-loven er å ivareta hensynet til personvernet.

Menneskerettsdomstolen: DNA, celleprøver og fingeravtrykk

En enstemmig menneskerettsdomstol fastslo i meldingsåret at England og Wales' praksis med å lagre DNA, celleprøver og fingeravtrykk til enkeltpersoner som er sjekket ut av straffesaker er i strid med menneskerettskonvensjonen.

Domstolen tolket Den europeiske menneskerettskonvensjonens (EMK) artikkel 8, en bestemmelse som stiller krav til at nasjonal lovgivning beskytter enkeltmennesker mot inngrep i privatlivet. Eventuelle inngrep i privatlivet må være lovhjemlede, rettmessige, forholdsmessige og nødvendige i et demokratisk samfunn.

Dommen gjelder to forhold. En gutt på elleve år ble arrestert og siktet for forsøk på ran. Det ble tatt fingeravtrykk og DNA-prøver fra ham. Han ble frikjent tre måneder senere. En voksen mann ble siktet for å ha trakassert sin partner, og måtte avgi fingeravtrykk og DNA. Saken ble henlagt etter at partneren ikke ønsket å forfølge saken videre. Begge de mistenkte bad om at opplysninger om fingeravtrykk og DNA-opplysninger måtte bli slettet fra registrene. Deres krav ble ikke etterkommet. Saken ble klaget videre, og ble til slutt behandlet av Menneskerettsdomstolens storkammer.

Domstolen uttrykker overraskelse over at engelsk og walisisk lov tillater uavgrenset lagring av DNA-opplysninger og fingeravtrykk fra personer som ikke er blitt dømt for noe. Domstolen påpeker at retten til beskyttelse av privatlivet vil bli svekket i en uakseptabel utstrekning om slike virkemidler tas i bruk uten en grundig avveiing mellom de mulige fordelene ved å bruke virkemidlene, og ulempene for privatlivet.

Prüm-samarbeidet – tilgang til databaser over DNA, fingeravtrykk og kjøretøyer

Mot slutten av meldingsåret ble det kunngjort at Norge har blitt enig med EU om å bli med i et forsterket politisamarbeid. Dette betyr at Norge vil innføre det såkalte Prüm-regelverket. Norsk politi får dermed tillatelse til å søke direkte i EU-landenes DNA-, fingeravtrykks- og kjøretøysregister ved etterforskning av kriminalitet. Dersom man får treff i en av disse databasene, skal man kunne be om å få mer informasjon utlevert. EU-landene får tilsvarende mulighet til å søke i norske registre.

Prüm-regelverket ble innført i EU i juni 2008 etter en rekordrask beslutningsprosess. Tilblivelsen av regelverket er blitt kritisert for å være udemokratisk og lite transparent. Opprinnelig ble samarbeidet iverksatt av et fåtall land på siden av EUs politiske organer etter terrorbombingen i Madrid i 2004. Initiativet ble tolket som et uttrykk for at flere EU-land synes utviklingen av politisamarbeidet innen EU gikk for sakte fremover. EU-parlamentet ble kun involvert på tampen av prosessen, og EUs ombudsmann for personvern, EDPS, ble ikke konsultert underveis, slik vanlig praksis er.

Når norske myndigheter nå knytter seg til dette samarbeidet, har Norge, så vidt Datatilsynet vet, ikke hatt mulighet til å påvirke regelverket på noe punkt i prosessen.

Fra et personvernperspektiv har Prüm-regelverket flere betenkelige sider. Formålet med utvekslingen av data er ikke presisert, det finnes ingen felles kriterier for hvordan DNA skal innhentes, og det mangler en beskrivelse av når opplysningene skal kunne søkes frem. Skal automatiserte søk på DNA-profiler i andre land kun tillates ved alvorlig kriminalitet, eller kan systemet også benyttes ved mindre forseelser?

Manglende harmonisering mellom reglene i de forskjellige landene er en annen innvending. Kriteriene for hvilke personer som skal registreres i de nasjonale DNA-databasene er høyst ulike fra land til land. Skal registeret kun baseres på materiale fra dømte, eller skal det inngå DNA fra andre personer, som for eksempel fra vitner eller mistenkte som senere ikke blir dømt? Storbritannia har Europas og verdens største DNA-register. Alle som pågripes i England og Wales får sitt DNA registrert i en database, uavhengig av om de blir dømt eller ikke. Mer enn fire millioner av landets innbyggere er registrert i DNA-registeret. I Norge kan politiet kreve at personer som er dømt til frihetsstraff avgir DNA til den nasjonale databasen. Se for øvrig også forrige avsnitt, *Menneskerettsdomstolen: DNA, celleprøver og fingeravtrykk.*

Den svenske FRA-loven

I meldingsåret vedtok den svenske Riksdagen en lov om signalspaning i forsvarets etterretningsvirksomhet (FRA-loven). Loven skal gi Forsvarets radioanstalt (FRA) hjemmel til å spane på elektronisk kommunikasjon som passerer den svenske riksgrensen.

Eksempel på slik elektronisk kommunikasjon er e-post, internett-tjenester og IP-telefoni. Det er ikke uvanlig at norsk innenlandsk elektronisk kommunikasjon rutes via Sverige, eller at inter-

nettrafikken mellom Norge og resten av verden går gjennom Sverige. Loven ble umiddelbart utsatt for sterk kritikk. Det ble blant annet hevdet at den bryter med viktige rettssikkerhetsprinsipper, samt Den europeiske menneskerettskonvensjonen (EMK) artikkel 8 og 10, bestemmelser som beskytter privatliv og ytringsfrihet. Fornyings- og administrasjonsdepartementet bad derfor Datatilsynet om å utrede lovens konsekvenser for personvernet i Norge.

FRA-loven representerer en markert endring i svensk sikkerhetspolitikk. Den vil fungere som en «elektronisk mur» langs den svenske riksgrensen. All elektronisk kommunikasjon skal passere gjennom definerte porter, der den blir gjenstand for automatisk skanning. Enkelte meldinger og samtaler vil bli valgt ut for nærmere undersøkelser på bakgrunn av bestemte søkekriterier. Forsvarets radioanstalt omtaler søkebegrepene de bruker for å sile ut meldinger som svært kompliserte, med tekniske og innholdmessige kriterier, uten å gå nærmere inn på hvordan de er konstruert.

Datatilsynet mener FRA-loven potensielt kan ha en nedkjølende effekt på ytringsfriheten. Muligheten for å bli overvåket kan medføre en usikkerhet som kan gjøre at enkelte vegrer seg for å kommunisere og innhente informasjon. I samhandling med hverandre tilpasser mennesker innhold og form etter kontekst og samtalepartner. En utenforstående og potensiell «medlytter» endrer forutsetningene for samhandlingen, også selv om samtalepartene «ikke har noe å skjule».

Meningsdannelse skjer ikke bare i den offentlige debatten, det skjer også i den private sfære. Der utvikles gjerne kritiske tanker, holdninger og perspektiver som kan utfordre det som der og da er alminnelig akseptert. Overvåking av privat kommunikasjon kan begrense rommet for meningsdannelse, og dermed legge en demper på prosesser som historisk har vist seg å være viktig for samfunnets utvikling.

Datalagringsdirektivet

Datalagringsdirektivet utløste mye debatt i løpet av året. Debatten var på sitt mest omfattende før sommeren. Saken førte til flere debatt- og leserinnlegg, ledere i landets største aviser, og artikler på blogger. Det ble endog etablert grupper mot innføring av direktivet på sosiale nettverk.

Datatilsynet har vært aktivt overfor media og publikum i denne saken, deltatt i debatter, holdt foredrag og skrevet avisinnlegg. En innføring av datalagringsdirektivet innebærer, etter Datatilsynets mening, et paradigmeskifte i det norske rettssystemet. Med en implementering i norsk rett, innfører man et etterforskningsmiddel som omfatter hele befolkningen, fullstendig uavhengig av borgerens eventuelle befatning med kriminelle aktiviteter.

Direktivet krever at trafikkdata for fasttelefon, mobiltelefon, bredbåndstelefoni, e-post og internettilgang, skal lagres. Innholdet i meldingene skal ikke lagres. Datatilsynet spør imidlertid om man vil stoppe der? Den svenske stat har, med virkning fra 2009, fastsatt FRA-loven som gir myndighetene anledning til å spane på innhold i elektronisk kommunikasjon som passerer riksgrensen. Målsetningen er å beskytte riket mot uønskede aktiviteter fra så vel statlige som ikke-statlige aktører.

Datatilsynet hadde forventet at regjeringen ville sende ut et forslag til implementering av direktivet i løpet av året. Så har ikke skjedd. Det er tydelig at regjeringen, enten på eget initiativ eller som følge av opinionen, har valgt å stille saken i bero.

Dersom lovgiver velger å implementere direktivet, er Datatilsynets subsidiære målsetning å arbeide for at færrest mulig opplysninger skal bli lagret i kortest mulig tid. Datatilsynet vil også påpeke at en eventuell innføring av direktivet vil kreve at det settes av betydelige ressurser for å kontrollere at trafikkdataene blir lagret sikkert.

Overføring av passasjeropplysninger til USA

USAs myndigheter krever en rekke opplysninger om flypassasjerer som kommer inn i amerikansk luftrom. Kravet om personopplysninger omfatter passasjerenes navn, kontaktopplysninger, reiserute, reisefølge og eventuell diett, og en rekke andre opplysninger. EU og USA har undertegnet en avtale om overføring av disse opplysningene. Artikkel 29-gruppen, et offisielt rådgivende personvernorgan i EU, gjennomgikk avtalen, og påpekte en rekke uklarheter som påvirker personvernet. Gruppen reagerte også på at ingen uavhengige tilsynsmyndigheter er tiltenkt rollen som kontrollør.

Norge er ennå ikke omfattet av avtalen når denne årsmeldingen leveres til Fornyings- og administrasjonsdepartementet. For at et flyselskap lovlig skal kunne utlevere passasjerinformasjonen fra Norge, må det derfor innhente samtykke fra passasjeren, eller søke Datatilsynet om dispensasjon fra forbudet mot å utlevere personopplysninger til stater som ikke sikrer et tilstrekkelig be-

skyttelsesnivå. Justisdepartementet og Utenriksdepartementet arbeider med å få til en avtale mellom USA og Norge.

Det er i meldingsåret gitt en konsesjon til Continental Airlines i påvente av den varslede avtalen.

9.1.4 Utlendingsfeltet

Utlendingsfeltet er stort og komplekst, med flere involverte parter som alle bidrar til behandlingen av personopplysninger. Utlendingsdirektoratet håndterer betydelige mengder sensitive personopplysninger i forbindelse med sin forvaltning av utlendingsloven. De samarbeider tett både med politiet og andre etater.

Datatilsynet kontrollerte i 2008 personvernforhold hos henholdsvis Utlendingsdirektoratet (UDI), Politiets Utlendingsenhet, Kripos og to asylmottak.

Et hovedtema for kontrollene hos UDI og Politiets Utlendingsenhet var håndteringen av fingeravtrykksregisteret EURODAC, hvilken informasjon asylsøkere får om registeret, samt metoder for alderstesting av barn. EURODAC er et europeisk register, opprettet for å forhindre at asylsøkere søker asyl i flere europeiske land. Registeret er strengt regulert, blant annet med full logging av tilgang, samt forbud mot å bruke opplysningene til andre formål.

Hos Kripos så Datatilsynet på håndteringen av fingeravtrykksregisteret AFIS, som også, i tillegg til EURODAC, innholder fingeravtrykk fra samtlige asylsøkere. Opplysningene i AFIS overføres til Kripos samtidig med at de samme fingeravtrykkene legges inn i EURODAC. AFIS ble tillatt brukt av politiet til etterforskning ved en lovendring i 2003.

Under tilsynene ble det tydelig at UDI utmerker seg ved at de har godt gjennomarbeidede rutiner for behandlingen av personopplysninger UDI selv har ansvaret for. Asylsøkere får dermed god informasjon om EURODAC. Det er Datatilsynets inntrykk at arbeidet med personvern og informasjonssikkerhet er godt forankret i ledelsen i direktoratet.

Datatilsynet observerte imidlertid ved tilsynet at asylsøkerne ikke fikk noen informasjon om fingeravtrykksregisteret AFIS, blant annet om at fingeravtrykkene de avgir senere kan bli brukt til etterforskning. Kripos har ansvaret for AFIS. UDI har ingen myndighet til å pålegge politiet å informere asylsøkerne.

Datatilsynet arbeider videre med saken i 2009.

9.2 Internett og telefoni

9.2.1 Internett

Domstolsavgjørelser på Internett

Datatilsynet har slått fast at publisering av rettsavgjørelser på Internett, både på åpne nettsteder og hos passordbeskyttede betalingsdatabaser, krever konsesjon fra Datatilsynet. Som følge av dette er det blitt behandlet konsesjonssøknader fra tre allerede etablerte aktører på området.

Tidligere var det kun stiftelsen Lovdata som systematisk publiserte dommer på nett. Lovdata har gjennom årene også bygget opp en betydelig kompetanse på å anonymisere dommer. I praksis har det vist seg at en tilstrekkelig anonymisering/avidentifisering av dommer er en ressurskrevende prosess, der rutiner og praksis kontinuerlig må oppdateres.

Materiale som er lagt ut på Internett vil i praksis være tilgjengelig og søkbart i uoverskuelig fremtid. En dom røper en historisk konflikt. Det å kunne, for alltid, bli koblet til en dom kan være svært belastende for de berørte partene, uavhengig av hvilken rolle man hadde i saken.

I meldingsåret skrev Datatilsynet til Domstolsadministrasjonen og anmodet om at den kunne bli med i et arbeid for å se på om det er mulig å legge anonymiseringen eller avidentifiseringen av dommer så nær domstolen som mulig, og om det kunne være aktuelt med lovhjemling eller retningslinjer. Utilstrekkelig anonymisert vil publisering av dommer kunne medføre store konsekvenser for de involverte partene.

Publisering av dokumenter på offentlige nettsider

Datatilsynet har de siste årene sett en rekke tilfeller der sensitive personopplysninger og fødselsnumre ved feil har blitt lagt ut på det offentliges nettsider. Denne tendensen fortsatte gjennom hele 2008. Det er først og fremst kommunale organer som legger ut slik informasjon i strid med personopplysningsloven.

Datatilsynet antar at den utvidete offentliggjøringen den nye offentleglova med forskrift legger opp til, vil føre til en økning i antallet personvernkrenkende publiseringer.

Det er nødvendig at den enkelte virksomhet forebygger at dokumenter blir lagt ut i strid med personopplysningsloven. For å begrense personvernkonsekvensene av ulovlige publiseringer har

Datatilsynet bedt berørte kommuner om å skjerme enkelte filer mot indeksering hos søkemotorene. Denne typen tiltak kan gjøres ved hjelp av enkle tekniske grep.

Datatilsynet understreker også behovet for å utarbeide gode retningslinjer for publisering på Internett før den offentlige elektroniske postjournalen tas i bruk i løpet av 2009.

Ærekrenkelser, ytringsfrihet og personvern

I 2008 ble det i en juridisk utredning fremsatt et forslag om å heve terskelen for hvilke ærekrenkelser som skal være straffbare etter straffeloven. Under det videre arbeidet med lovendringsforslaget falt Justis- og politidepartementet ned på at det ønsket å gå enda lenger enn det forslaget la opp til, og foreslo at bestemmelsen i stedet skal fjernes fra straffeloven. Datatilsynet fant det vanskelig å støtte forslaget ut fra den fremlagte utredningen og høringsbrevet, og viste til manglende utredning av forholdet til Internett og andre elektroniske kanaler. Å avkriminalisere ærekrenkelser innebærer at én av skrankene for publisering av krenkende ytringer på Internett fjernes. Selv om det fortsatt skal være mulig å gå til sivilt søksmål, vil avkriminaliseringen lett kunne oppfattes som en liberalisering i forhold til hva som kan publiseres.

Med Internett har en ærekrenkelse fått større skadepotensial enn før. Kraftige, sofistikerte søkemotorer i kombinasjon med stadig økende lagringskapasitet, gjør at et ubegrenset antall personer får tilgang over et langt, ubestemt tidsrom. Datatilsynet ble i 2008 kontaktet av en rekke personer som ufrivillig er eksponert på Internett, og som ber om hjelp til å få opplysningene fjernet. Avgjørelser i Personvernnemnda tyder på at retten til å ytre seg på nett er svært vid, selv om ytringene oppfattes som svært inngripende og krenkende for den omtalte.

Datatilsynet utelukker ikke at det på dette området kan etableres «selvreguleringsordninger» som likner Pressens faglige utvalg (PFU). Personvernkommisjonen har i løpet av meldingsåret foreslått at det opprettes en nettnemnd som kan behandle klager fra personer som mener seg utsatt for krenkende ytringer på Internett.

Det foregår nå et arbeid for revisjon av personopplysningsloven. I denne forbindelsen har Datatilsynet påpekt behovet for å se på barns personvern spesielt. Barns personvern kan bli skadelidende dersom det ikke lenger skal være aktuelt for politiet på eget initiativ å ta opp saker der barn blir utsatt for sterkt ærekrenkende ytringer.

Datatilsynet har i 2008 arbeidet med saker der interesseorganisasjoner eller talerør for systemkritikk bruker nettpublisering for å underbygge sine påstander om myndighetsmisbruk fra barnevernets side. I disse sakene har det blant annet vært publisert svært sensitive dokumenter, som for eksempel beretninger fra foreldre, ikke-anonymiserte dommer og psykolograpporter.

Tilgjengeliggjøring av kulturarven på nett

Datatilsynet har i 2008 mottatt henvendelser fra både Riksantikvaren og universitetsmuseene angående tilgjengeliggjøring av deler av de digitale samlingene på nett. I forhold til publisering av universitetsmuseenes digitale samlinger skriver Kunnskapsdepartementet i St.meld. nr. 15 (2007-2008) *Tingenes tale* at museene har ansvar for å tilrettelegge og tilgjengeliggjøre egne data, men at overordnede rammer må være på plass før dette skjer.

Datatilsynet har forståelse for ønsket om å publisere materialet for forskere, forvaltere og allmennheten. Samtidig må Datatilsynet påpeke en rekke problemstillinger i forhold til den enkeltes personvern. Publisering fordrer at materialet er vurdert opp mot personopplysningslovens grunnkrav. Datatilsynet har i de aktuelle sakene kommet fram til at en begrenset publisering vil være i samsvar med personvernlovgivningen.

Søkemotorer

De viktigste verktøyene for informasjonsinnhenting på Internett er søkemotorene, og den mest kjente av dem er utvilsomt Google. Slike søkemotorer benyttes av så å si alle – både privat og i jobbsammenheng.

Våren 2008 kom Artikkel 29-gruppen med en uttalelse om rettslige problemstillinger knyttet til søkemotorene generelt, og til Google spesielt. Arbeidsgruppen slår blant annet fast at personverndirektivet gjelder dersom søkemotorene tilbyr tjenester til brukere i EØS-land, selv om hovedkvarteret til virksomhetene ligger utenfor EØS-området. Google er ikke enig i at loven kommer til anvendelse, og ønsker å holde tilbake data i seks måneder utover den foreslåtte slettefristen til arbeidsgruppen. Videre uttaler Google at IP-adresser ikke kan anses for å være personopplysninger. For øvrig er selskapet velvillig innstilt overfor vi-

dere samarbeid med de europeiske myndigheter innenfor området.

Datatilsynet må ta stilling til flere av de ovennevnte spørsmålene i forbindelse med den kommende inkluderingen av enkelte norske byer i tjenesten Google Street View i Googles karttjeneste Google Maps. En liknende sak vedrørende et norsk selskap er for øvrig under behandling. Sakene reiser særskilte spørsmål om anonymisering av avbildede personer, samt anvendelsen av personopplysningslovens grunnkrav på de deler av tjenesten som innebærer en behandling av personopplysinger.

Oppslagsverk

Wikipedia er en annen internettbasert tjeneste som er mye brukt. Her er det brukerne selv som legger inn informasjon i oppslagsverket. Selv om nettstedet har en personvernpolicy, og det finnes retningslinjer for redigering og kvalitetssikring av opplysningene, oppstår det nødvendigvis enkelte personvernrelaterte spørsmål. Som eksempel kan nevnes en side som inneholder en liste over personer tatt for doping. Her figurerer blant annet en rekke navn på norske idrettsutøvere som trolig ikke har fått noen mulighet til å forsvare seg mot påstandene.

Fildeling

Advokatfirmaet Simonsen fikk i 2008 fornyet konsesjonen om registrering av aktivitet på ulike fildelingsnettverk. Konsesjonen omfatter blant annet loggføring av IP-adresser. Advokatfirmaet sendte ut en henvendelse til norske internettilbydere med oppfordring om videreformidling av tilståelsesbrev til nettbrukere som kunne mistenkes for å ha deltatt i fildeling. Tilsynet var raskt ute med å påpeke at en slik praksis trolig vil være i strid med etablerte rettssikkerhetsgarantier og grunnleggende menneskerettigheter, deriblant det såkalte selvinkrimineringsforbudet.

Nettsamfunn

Bruken av nettsamfunn slik som Facebook, Nettby og YouTube har økt i 2008. Særlig yngre personer er aktive brukere av slike internettbaserte samlingssteder. Mange av brukerne er åpne om egen identitet. Denne åpenheten er tilsiktet i og med at formålet med bruken av tjenesten ofte er kontakt med venner og nettverksbygging. Ved å knytte egen profil til andres dannes store sosiale nettverk med betydelig mengder personlig informasjon. Materialet som publiseres er ikke bare knyttet til egen identitet. Mange publiserer bilder av andre personer, eller personopplysninger knyttet til andre, uten at de først har innhentet samtykke fra den det gjelder. Selv om materialet ofte publiseres i en lukket krets, har Datatilsynet fått en rekke henvendelser vedrørende kopiering og bruk av informasjonen i andre sammenhenger. Datatilsynet tror det finnes et gap mellom hva brukerne av nettsamfunnene tror om beskyttelsesnivået for opplysningene, og hvilken beskyttelse opplysningene faktisk er underlagt. For flere av nettsamfunnenes del, og ikke minst Facebook og YouTube, er det videre en utfordring at nettsamfunnene ligger utenfor Norge.

9.2.2 Tilsyn rettet mot internett, tele- og epostleverandører

Tilsyn hos internettleverandører og teleoperatører

Etter tips om brudd på sletteplikten hos internettleverandører (ISP-er) og teleoperatører, kontrollerte Datatilsynet håndtering av trafikkdata hos fem virksomheter.

Datatilsynet er opptatt av at elektronisk kommunikasjon skal skje på en måte som gir et tilfredstillende personvern. Kunnskap om personverntilstanden på området er svært viktig fordi Stortinget etter hvert skal ta stilling til om Norge skal implementere datalagringsdirektivet, noe som vil kunne medføre ytterligere utvidelser i lagringen av trafikkdata.

Tilsynene viste at noen leverandører overtrådte regelverket, mens andre aktører hadde gjort mindre forseelser. De fleste leverandørene hadde mangler ved sine internkontrollsystemer. Dette gjaldt for eksempel mangel på rutiner for innsyn, retting og sletting. Imidlertid hadde én leverandør, den samme som i 2007 opplevde en større datalekkasje, lagt ned et betydelig arbeid i å lage et tilfredsstillende internkontrollsystem.

Flere leverandører hadde ikke inngått tilstrekkelige avtaler med sine databehandlere. Slike avtaler skal sikre at rettigheter og plikter blir ivaretatt, selv om eksterne databehandlere står for håndteringen av opplysningene. Det var gjennomgående mangel på sletting i alle virksomhetene.

Noen leverandører hadde mangelfull sikkerhet på sine påloggingssider for kunder. Passord for e-postløsninger og passord for kundesidene

(«Min side») forekom ukryptert og ikke tilstrekkelig beskyttet mot at virksomhetens ansatte kunne skaffe seg urettmessig tilgang.

Tilsyn hos leverandører av e-post

Datatilsynet kontrollerte håndtering, sikring og sletting av e-post og SMS-kommunikasjon hos fem leverandører. Tre tilsyn fant sted hos e-postleverandører og to hos leverandører av SMS-tjenester.

Datatilsynet observerte at det foregikk en utbredt lagring av innhold i elektronisk kommunikasjon hos tilsynsobjektene. En tilbyder av e-post og en tilbyder av SMS lagret kommunikasjonen på ubestemt tid.

Kundene ble ikke gjort oppmerksomme på at innholdet i e-postene deres ble lagret i sikkerhetskopier uforholdsmessig lenge. Generelt ble det hos alle leverandørene gitt mangelfull informasjon til kunden om hva som skjer av lagring, sletting, innsyn og retting.

Tilsynene avdekket at leverandørene gjennomgående hadde liten kunnskap om personopplysningsloven.

Datatilsynet avdekket også noe mangelfull informasjonssikkerhet hos tilsynsobjektene, spesielt manglet kryptering av passord hos en enkelt leverandør. Alle leverandørene hadde mangler i forhold til kravet om et systematisk arbeid med internkontroll.

Det fantes også manglende rutiner for utlevering av personopplysninger. De fleste leverandørene opplevde at de hadde en samfunnsmessig plikt overfor politiet til å oppbevare opplysninger som senere kan komme til anvendelse i etterforskning. Flere leverandører uttrykte usikkerhet om forholdet mellom personopplysningsloven og politiets ønsker.

9.2.3 Vanskelig autentisering på Internett

Et gjennomgående problem med elektronisk samhandling er autentiseringen av de kommuniserende partene. Løsningene som benyttes i dag, gir i mange tilfeller ikke tilstrekkelig trygghet for at samhandling skjer med rette vedkommende. For den enkelte innbygger innebærer dette at det eksisterer en mulighet for at løsningene kan kompromitteres, at uvedkommende kan handle på vedkommendes vegne, eventuelt at informasjonen kan leses av uvedkommende.

9.2.4 Telefoni

Konsesjoner til teletilbydere

Datatilsynet har gjennom tilsyn og ordinær saksbehandling avdekket at enkelte teletilbydere har liten kunnskap om personvernlovgivningen. Selv om teletilbydere sjelden behandler sensitive personopplysninger, er mengden opplysninger de lagrer om hver enkelt så omfattende at virksomhetene likevel er underlagt konsesjonsplikt. Dette var ukjent for flere teletilbydere. Den manglende kunnskapen om personvernlovgivningen er særlig betenkelig sett i sammenheng med den omfattende lagringen av personopplysninger som Datalagringsdirektivet legger opp til.

Ung1881.no – automatisk oppdatering av opplysningstjeneste

Personvernnemnda fattet i 2008 en avgjørelse om at nettstedet ung1881.no ikke automatisk kunne oppdatere sin opplysningstjeneste med opplysninger om den personen som disponerte et gitt telefonabonnement når brukeren av mobiltelefonnummeret er en annen enn den abonnementet står registrert på. Slik oppdatering kan kun gjøres etter samtykke fra abonnenten. Personvernnemnda opprettholdt følgelig Datatilsynets vedtak.

9.3 Altinn, skattedirektoratet og utenrikstjenesten

9.3.1 Tilsyn hos Altinn og Skattedirektoratet

Datatilsynet påla Altinn sentralforvaltning og Skattedirektoratet å utbedre flere punkter ved Altinn-portalen etter et tilsyn mai 2008.

Altinn tilbyr en felles påloggingsløsning, der brukeren kan samhandle med flere statlige virksomheter via samme portal. Både virksomheter og privatpersoner kan levere inn pliktige oppgaver, som momsoppgave og selvangivelse. Man kan også signere gjeldsbrev fra Lånekassen for utdanning.

Kontrollen avdekket en del forhold Datatilsynet ser som kritikkverdige. Gjennom tjenesten Altinn tilbyr flere store offentlige aktører kundekontoer til publikum, uavhengig av om den enkelte ønsker det eller ikke. Kontoene fylles med informasjon fra ulike behandlingsansvarlige. Etter tilsynets vurdering er en slik praksis problematisk. Individuell valgfrihet blir satt til side, sammen med muligheten til selv å ta stilling til om løsningene tilbyr tilfredstillende sikkerhet. Den felles påloggingsløsningen bruker fødselsnummer og

pin-koder fra selvangivelsen som brukernavn og passord. Datatilsynet har tidligere uttalt seg kritisk til at påloggingsinformasjonen sendes i åpne postsendinger over et kort, kjent tidsintervall. Metoden innebærer risiko for misbruk.

Disse punktene ble krevd utbedret etter tilsynet:

- Distribusjonskanalene for brukernavn og passord må gjøres tryggere.
- Det må fremskaffes lovgrunnlag dersom man skal fortsette å opprette kontoer for alle landets innbyggere uten deres samtykke.
- Det må godtgjøres at det finnes hjemmel for å tilgjengeliggjøre selvangivelser uoppfordret.
- Altinn må avstå fra unødvendig mellomlagring og opprettelse av uformaliserte elektroniske arkiv.

Altinn og Skattedirektoratet har klaget på vedtaket.

9.3.2 Utenrikstjenesten

Datatilsynet gjennomførte våren 2008 kontroller hos Utenriksdepartementet (UD), ved ambassadene i Moskva, London og Ankara. Det ble i tillegg gjennomført et innledende møte med UD i Oslo.

Temaet for kontrollene var departementets behandling av personopplysninger, særlig i forbindelse med søknader om visum, oppfølging av norske statsborgere i landet og personundersøkelser/verifiseringsrapporter (konsulære saker).

Valg av destinasjoner var begrunnet i ønsket om å få et dekkende bilde av utenriksstasjonenes behandling av personopplysninger. Dette forutsatte valg av utenriksstasjoner med ulik størrelse, geografisk plassering, antall søknader om visum, asyl og familiegjenforening, og antall personer med norsk statsborgerskap i landet. En vesentlig del av arbeidet ved ambassadene involverer ikke behandling av personopplysninger. Antall medarbeidere ved de kontrollerte ambassadene varierte fra 50 i Moskva til 15 i Ankara. Det var omtrent like mange lokalt ansatte som utsendte fra Norge.

Utenrikstjenesten gir norske statsborgere råd og hjelp overfor utenlandske myndigheter, personer og institusjoner. Blant oppgavene er bistand i forbindelse med straffeforfølging, ulykker, sykdom og dødsfall. Slike oppgaver medfører at Utenrikstjenesten må behandle sensitive opplysninger om enkeltmennesker.

Utenrikstjenesten gjør også oppgaver for Utlendingsdirektoratet, Utlendingsnemnda og Politidirektoratet. UD mottar blant annet søknader om visum og utstedelse av pass. Informasjon utveksles for øvrig med Arbeids- og inkluderingsdepartementet, Justisdepartementet, NAV, Skattedirektoratet, politiet, barnevernet, sykehus, pårørende og forsikringsselskaper. I tillegg kommer instanser i landet der utenriksstasjonen er lokalisert.

På generelt grunnlag har Datatilsynet et positivt inntrykk av Utenriksdepartementet og utenrikstjenestens ivaretakelse av personvern. Allerede før kontrollen ble varslet var det igangsatt en prosess for vurdering av rutiner, og endring av disse. Praktisk tilrettelegging i forbindelse med gjennomføringen av kontrollene var svært god, både fra UD sentralt og utenriksstasjonenes side.

Funn under kontrollene var i det vesentlige knyttet til internkontrollplikten i personopplysningslovens § 14 og informasjonssikkerhet etter § 13.

Når det gjelder informasjonssikkerhet var funnene i hovedsak knyttet til manglende etterlevelse av systempliktene i regelverket, det vil si at departementet ikke hadde gjort de vurderinger de selv plikter å gjennomføre, samt at de ikke hadde etablert nødvendige rutiner i organisasjonen hva gjelder sikring av personopplysninger.

Som flere innen offentlig forvaltning, synes ansatte ved ambassadene å benytte ubeskyttet e-post relativt ukritisk. Usikret e-post ble brukt til å kommunisere om enkeltpersoner med etater som Utlendingsdirektoratet, politiet og NAV. Dette er ikke en praksis UD alene kan ses som ansvarlig for. En samlet offentlig forvalting har ikke implementert nødvendig infrastruktur for tilfredstillende sikker samhandling. At moderne norsk forvaltning kommuniserer opplysninger om enkeltpersoner over ubeskyttet e-post, er etter tilsynets oppfatning svært uheldig.

9.4 Barn og unge i barnehage og skole

9.4.1 Ny veileder: Bilder av barn på Internett

Det er et klart behov for at personalet i barnehager og skoler får en økt bevissthet om personvern generelt, og om publisering av bilder spesielt. Det blir publisert bilder i enorme mengder på åpne sider som hvem som helst har tilgang til.

Datatilsynet laget i 2008 en veileder om bilder av barn på Internett. Veilederen er primært rettet mot skoler og barnehager, men også foreldre og idrettslag er aktuelle målgrupper. Bakgrunnen for prosjektet er den stadig økende publiseringen av bilder av barn på nett. Mange publiserer bildene

på sider man må ha brukernavn og passord for å komme inn på, og tror at bildene da er godt beskyttet. Men hvor ofte skiftes passordet? Og kan man egentlig stole på at de andre foreldrene behandler bildene som de skal? Flere barnehager brenner dessuten CD-er med bilder av alle barn til alle familier uten å vurdere om bildene er egnet til slik masseproduksjon.

Samtykkeskjemaene foreldrene får ved barnehage- / skolestart om fotografering er ofte svært mangelfulle. Og selv om en publisering kan være lov, er den alltid etisk riktig? Er situasjonen positiv og viser hva barn kan og vil, eller negativ og viser barn som er lei seg eller som føler at de mislykkes i en situasjon? Ville vi selv som voksne like å bli fremstilt slik på nettet?

Barna i dag blir tatt bilde av både hjemme, i barnehagen, på skolen og på fritidsaktivitetene, og alle forbeholder seg retten til å publisere bilder på nett uten at barna skal høres. Hvordan skal disse barna bli mottagelige for opplæring i nettvett, når de fra den dagen de er født opplever at voksne nærmest teppelegger Internett med bilder av dem – uten å spørre, og ofte uten noen form for vurdering på forhånd?

Veilederen er bygd opp rundt intervjuer med personer som har ulike innfallsvinkler til nettpublisering; Barneombudet, en etterforsker i Kripos, en pedagog, en forelder og en ungdom. Hvert intervju avsluttes med noen tommelfingerregler og diskusjonsoppgaver. Det er også med en del konkret fakta, slik som hva lovverket og barnekonvensjonen sier.

9.4.2 Tilsyn: Data i skolen

Enkelte skoler ønsker å kontrollere det som skjer på skolens datanettverk og på hver enkelte elevs datamaskin. Andre skoler har valgt løsninger med minimal kontroll, og foretar isteden en enkel, generell filtrering av tilgang.

I meldingsåret gjennomførte Datatilsynet to kontroller ved videregående skoler.

De to skolene ga ikke skriftlig informasjon til brukerne om hvordan IKT-verktøyene ble håndtert. Instruksene for bruk av skolenes IKT-verktøy var ikke tilfredsstillende, og det var heller ikke etablert en tilstrekkelig internkontroll. Sletting av informasjon på servere og i sikkerhetskopier etter at formålet med lagringen var oppnådd var også utilstrekkelig.

Begge skolene var bekymret for at enkelte elever benyttet skolens IKT-verktøy til ulovlig eller uønsket virksomhet. Det var likevel stor forskjell på hvordan IKT og personvern ble håndtert ved de to kontrollobjektene. Den ene skolen hadde valgt betydelig mindre personverninngripende måter å løse sitt kontrollbehov på enn den andre skolen. Den skolen som i størst grad åpnet for at IKT-verktøyet skulle kunne benyttes fritt av brukerne, mente at læringsverdien oversteg ulempene med tanke på mulig «ulovlig» bruk.

9.4.3 Tilsyn: Bruk av læringsverktøy i skoler

Utdanningsinstitusjonene har i økende grad tatt i bruk elektroniske læringsverktøy i sitt undervisningsopplegg. Læringsverktøy gir muligheter for overvåking av elevene, og til dels lærerne, i et omfang som tidligere ikke har vært mulig. Datatilsynet så på bruken av slike læringsverktøy i 2005, og konkluderte med at det var naturlig å følge opp med ytterligere tilsyn.

Som en følge av dette gjennomførte Datatilsynet i 2008 fem kontroller med fokus på læringsverktøy i skoler. Tre kontroller ble gjennomført ved videregående skoler og to av kontrollene var rettet mot fylkeskommuner, som behandlingsansvarlig for skolene. Skolene brukte læringsverktøyene *It´s learning* og *Fronter*.

Spesielt ble det rettet fokus mot den informasjonen brukerne får, og hvor lenge opplysningene i systemene lagres. Datatilsynet så videre på sikkerheten i systemene, samt i hvilken grad systemet også ble benyttet til overvåking av brukerne.

Tilstanden var langt bedre enn forventet. Med bakgrunn i erfaringen fra kontrollene i 2005 hadde Datatilsynet forventet å avdekke flere brudd på bestemmelsene i personopplysningsloven. To gjennomgående funn var likevel alvorlige. Kontrollene avdekket at verken elever, lærere eller foresatte får tilfredsstillende informasjon om læringsverktøyene. Det viste seg også at det ikke fantes sletterutiner for personopplysninger.

Datatilsynet konkluderte under kontrollene også med at skoler som benytter plagiatkontroll for å avdekke juks, må anonymisere tidligere innleverte elevoppgaver som inngår i referansedatabasen.

Læringsverktøyet som kommunikasjonskanal

Læringsverktøyene er laget for at læreren skal kunne kommunisere med eleven. Datatilsynet oppdaget at systemet i tillegg blir benyttet som en informasjonskanal mellom skolen og lærerne, skolen og foreldrene, lærerne imellom, og i enkelte tilfeller, elevene imellom.

En funksjon i systemet gjør det mulig for administratoren av en gruppe eller et rom å se hvem som har lest hvilke dokumenter. Datatilsynet har mottatt klager fra lærere som føler seg overvåket ved at skolens ledelse kan se når og om et dokument er lest. Datatilsynet har ikke varslet pålegg om at denne funksjonen skal fjernes, men har påpekt at den bør være avskrudd dersom systemadministratoren ikke har et saklig behov for å vite hvem som har lest dokumentene.

9.4.4 Forskning på barn og unge

Kommunale ungdomsundersøkelser

Gjennom en henvendelse fra foreldrerådets arbeidsutvalg (FAU) ved Rugtvedt ungdomsskole i Bamble ble Datatilsynet gjort oppmerksom på at kommunen hadde gjennomført en omfattende spørreundersøkelse blant elevene på ungdomstrinnet. Undersøkelsen var gjennomført i samarbeid med Høgskolen i Telemark.

Elevene hadde besvart et meget omfattende spørreskjema. Mange av opplysningene som elevene hadde avgitt var av svært sensitiv karakter, og vedrørte blant annet helseforhold og seksuell legning. Elevene besvarte også spørsmål av selvinkriminerende karakter om egen medvirkning til konkrete straffbare forhold som hærverk og vold.

Datatilsynet påla kommunen å anonymisere eller slette opplysningene. Bakgrunnen for pålegget var at elevene hadde avgitt opplysningene basert på uriktige forutsetninger. Elevene hadde på forhånd blitt informert om at opplysningene ville bli behandlet anonymt. Imidlertid var opplysningene, selv om de ikke inneholdt navn eller andre direkte identifiserende kjennetegn, så omfattende at man likevel ville kunne identifisere mange av elevene. Datatilsynet mente det kan stilles spørsmål ved om elevene selv evner å overskue konsekvensene av å delta, og at de foresatte derfor burde ha samtykket til undersøkelsen.

Opplysningene ble bekreftet anonymisert i tråd med Datatilsynets vedtak.

Høring: Innføring av et sentralt elevregister for forskning

I høringsbrev av 20. juni 2008 fremmet Kunnskapsdepartementet forslag om endringer i grunnskoleloven og Lov om videregående opplæring. Det ble foreslått å opprette et sentralt register for alle elever i grunnopplæringen.

Det opplyste formålet med registeret er «å leggje til rette for analysar, statistikk og forskning om læringsutbytte, læringsmiljø og lærarkompetanse til bruk for kvalitetsutvikling og kvalitetskontroll innen grunnopplæringa.»

Den foreslåtte lovendringen vil gi hjemmel for en sentral registrering av identifiserbare, detaljerte og til dels sensitive opplysninger om hele den oppvoksende befolkningen. Dette inkluderer opplysninger om sosiale og helsemessige forhold, religiøs oppfatning, seksuell legning og etnisk tilhørighet. Opplysningene skal kunne lagres i uoverskuelig fremtid. Bestemmelsen vil også gi hjemmel for å koble opplysningene med ulike ikke-spesifiserte registre. Det endelige omfanget av registreringen blir derved umulig å forutse.

Datatilsynet uttalte seg svært negativt til forslaget. Et personregister som foreslått vil etter Datatilsynets vurdering være ett av de mest personverninngripende registrene som er etablert i Norge – sett med hensyn til opplysningenes art og omfang, koblingsmuligheter, lagringstid og rettslig grunnlag. Misbrukspotensialet vil kunne være svært stort.

Høringsnotatet berører ikke alternative metoder for å skaffe nødvendig kunnskap for å bedre kvaliteten på opplæringen, og vurderer heller ikke om formålet kan nås gjennom tradisjonell samtykkebasert forskning.

I den påfølgende mediedebatten hevdet Kunnskapsdepartementet at det ikke hadde ment å gå så langt som det den foreslåtte hjemmelen legger opp til.

Datatilsynet erfarer imidlertid stadig at registre som er etablert for ett konkret og avgrenset formål ofte tas i bruk for nye formål som aktualiseres etter noen tid. Når opplysningene først er registrert, er terskelen for å bruke dem til nye, mer eller mindre aktverdige formål, svært lav.

9.5 Identitet og biometri

9.5.1 Det fremtidige folkeregisteret

I meldingsåret tok Datatilsynet stilling til rapporten *Utveksling av grunndata på personinformasjonsområdet.* Rapporten handler om den fremtidige utformingen av folkeregisteret. Datatilsynet mener rapporten er ensidig, og ikke bør bli lagt til grunn for et eventuelt forslag om lovendringer.

Folkeregisteret legger viktige premisser for personverntilstanden i Norge i mange år fremover. Tilsynet påpeker spesielt at det ikke bør registreres flere eller andre opplysninger i folkeregisteret enn i dag, at enkelte av de opplysningene

som i dag registreres i folkeregisteret bør utgå, og at fødselsnummeret (eller en eventuell ny identifikator) ikke bør bli gjort mer tilgjengelig enn i dag.

Rapporten bygger på enkelte grunnleggende forutsetninger som det kan være grunn til å stille spørsmål ved, skriver Datatilsynet i sin høringsuttalelse. For eksempel synes gruppen ukritisk å legge til grunn at det «nye» folkeregisteret vil komme i stedet for en rekke lokale registre, for eksempel innen de ulike forvaltningsorganene. Datatilsynet deler ikke gruppens tro på at opplysningene ikke også vil bli registrert lokalt. Dessuten anser Datatilsynet at det enkelte offentlige organ nettopp bør ha egne registre, spesielt tilpasset sitt eget behov. Når ett register skal ivareta flere organers ulike behov, vil registeret som sådan fort bli altfor omfattende for det konkrete behovet hvert enkelt organ har. Dette vil på sikt kunne medføre en unødvendig spredning av personopplysninger.

Datatilsynet er redd for at ansvaret for folkeregisteret pulveriseres. Den foreslåtte modellen legger opp til at mange parter har ansvar for å sørge for at registeret til enhver tid er oppdatert og korrekt. Hvem som bærer det endelige ansvaret for uriktige folkeregisteropplysninger blir etter dette uklart.

9.5.2 Biometri

Datatilsynet observerer at flere ønsker å ta i bruk biometri i ulike løsninger. Biometriske løsninger fremstår for mange brukere som enkle og praktiske, samtidig som de hevdes å gi god sikkerhet. Datatilsynet opplever at fingeravtrykk benyttes i økende grad, ikke nødvendigvis for å bedre autentiseringssikkerheten, men for å oppnå rask behandling uten at personell er tilstede. Alternativene fremstår som tungvinte og velges bort av effektivitetshensyn. Folk flest ser ut til å være relativt positive til biometriske sikkerhetsløsninger. Det kan skyldes at de ikke er kjent med de mulige negative sidene.

Biometriske data er varige, entydige identifikatorer. Personvernregelverket krever at slike unike identifikatorer bare benyttes når det er nødvendig for å gi tilstrekkelig sikkerhet, og alternativene ikke er egnet.

Datatilsynet var på tre kontroller av biometriske løsninger i 2008. Kontrollene avdekket at det ikke var blitt foretatt vurderinger av om det fantes andre løsninger som kunne brukes i stedet for biometriske data.

Alle tilsynsobjektene benyttet templates, ikke hele bilder av fingeravtrykk. Når man bruker en template bruker man informasjon fra utvalgte punkter i fingeravtrykket, ikke informasjon fra hele avtrykket. Dette reduserer personvernulempene noe. Ingen av tilsynsobjektene hadde foretatt nødvendige risikovurderinger av om den valgte løsningen var god nok til å kunne autentisere personer på en sikker måte. Det var heller ikke foretatt risikovurderinger av om sikkerheten i løsingen var tilstrekkelig.

9.6 Arbeidsliv

Samarbeid med LO

Det samles inn stadig mer informasjon om den enkelte i et arbeidsforhold. Styrkeforholdet mellom partene, for eksempel ved en oppsigelse, er over tid blitt endret i arbeidsgivers favør. LO har satt ned en arbeidsgruppe for å se på disse problemene.

Datatilsynet har vært med på et innledende møte med arbeidsgruppen, holdt flere foredrag i samarbeid med FAFO og LO, samt gitt skriftlige innspill til arbeidet.

Den nylige publiserte FAFO-rapporten, «*Personvern under press – hvor går grensene i arbeidslivet*», er det foreløpige resultatet av arbeidet. LO skal jobbe videre med disse utfordringene. Datatilsynet synes det er positivt at fagforeningene nå setter fokus på personvernproblematikken i arbeidslivet og ønsker å bidra videre i dette arbeidet.

9.6.1 Tilsyn hos bedriftshelsetjenesten

Datatilsynet var i meldingsåret på kontroll hos fire virksomheter for å se på behandling av personopplysninger i bedriftshelsetjenesten.

Bedriftshelsetjenesten er en sentral medspiller for ivaretakelsen av arbeidstakeres helse på arbeidsplassen. Arbeidsområdet omfatter både fysiske og psykososiale forhold.

I kontrollene så Datatilsynet på virksomhetenes behandling av helseopplysninger, om opplysninger eventuelt blir utlevert til arbeidsgiveren, og hva slags informasjon de ansatte får.

På bakgrunn av tidligere mottatte klager så Datatilsynet spesielt på rutiner knyttet til gjennomføring av arbeidsmiljøundersøkelser, herunder hvordan arbeidstakernes anonymitet ble ivaretatt i oppsummeringsrapporter fra undersøkelsene.

Alle virksomhetene hadde gode rutiner for håndtering av helseopplysninger i praksis, men flere av rutinene var ikke tilstrekkelig dokumentert i bedriftens internkontrollsystem. Ingen virksomheter utleverte helseopplysninger om arbeidstakerne til arbeidsgiveren uten forutgående samtykke og informasjon. Tre virksomheter hadde ikke sendt inn melding om behandling av personopplysninger til Datatilsynet. En virksomhet hadde personvernombud, og var fritatt fra meldeplikt. Informasjonssikkerheten var gjennomgående god.

Datatilsynet har hittil stilt krav om at bedriftshelsetjenester som tilbyr legetjenester ut over de krav arbeidsmiljølovgivningen stiller, skal skille mellom opplysinger som er relevante for bedriftshelsetjenesten og andre opplysninger. Opplysninger knyttet til et individuelt helsetjenestetilbud ut over bedriftshelsetjenesten, skal inngå i en egen pasientjournal. Kontrollene viste at de virksomhetene som tilbød slike ekstra helsetjenester, holdt de ulike opplysningstyper atskilt. Det viste seg imidlertid at dette skillet ikke alltid var like lett å opprettholde i praksis. Av hensyn til pasientenes helse og sikkerhet ble det i stor grad ansett nødvendig å føre «dobbel journal»; viktige helseopplysninger fra bedriftshelsetjenesten måtte også føres i den private journalen, slik at det ble dannet et riktig og helhetlig bilde av pasientens helsetilstand. Datatilsynet vil følge opp saken videre med helsemyndighetene.

9.6.2 Gjennomgang av regelverket om vaktvirksomhet

I meldingsåret ga Datatilsynet et høringssvar til en rapport fra en arbeidsgruppe med et mandat som blant annet har vært å styrke rettssikkerheten for personer som kommer i kontakt med vaktbransjen.

Det tydeliggjøres i forslaget at den som utøver vakttjeneste ikke har særlig adgang til å bruke fysisk makt mot personer utover det enhver har adgang til. Datatilsynet støtter arbeidsgruppens tolkning av at dette må omfatte både publikum og personer som er ansatt som vektere.

Datatilsynet mener imidlertid at andre forslag i rapporten vil kunne medføre svært store inngrep i vekternes krav på rettssikkerhet og personvern. Spesielt vil dette gjelde den omfattende adgangen til å innhente utvidet politiattest, både for vektere og «personer med vesentlig innflytelse» over driften av vaktselskapet. Utvidede politiattester inneholder opplysninger om henlagte og verserende straffesaker. I tillegg legger forslaget opp til at man kan sjekke vandelen til nærmeste familie, og at det skal opprettes et vaktvirksomhetsregister som blant annet skal inneholde meldinger om mistanke om straffbare forhold blant vekterne. Datatilsynet anbefaler i høringen at flere av forslagene utredes nærmere, slik at personvernproblemer, og tiltak for å imøtegå disse, klargjøres.

9.7 Idrett

Kampen mot doping er et eksempel på at et aktverdig formål kan helliggjøre et middel, uten at det stilles spørsmål ved de følgene et tiltak vil kunne få for den enkeltes personvern.

For Datatilsynets arbeid med disse spørsmålene har én av utfordringene vært at toppidretten er underlagt et internt regelverk som håndheves av nasjonale og internasjonale organisasjoner. Dette regelverket er norske utøvere forpliktet til å følge dersom de ønsker å konkurrere internasjonalt. Det er opplagt at norsk lov, herunder personopplysningsloven, rettslig sett har større tyngde enn idrettens eget regelverk. I praksis vil imidlertid Datatilsynet ha begrensede muligheter til å sette ned foten fordi konsekvensen vil kunne være at norske utøvere nektes deltakelse i internasjonale konkurranser. Datatilsynet bestrider ikke at en toppidrettsutøver må akseptere å leve under et strengt kontrollregime, men er av den oppfatning at grensen for hva utøverne må leve med er nå passert.

Trolig som følge av den intensiverte kampen mot doping innenfor toppidretten har terskelen for hvem som skal kunne kontrolleres blitt senket. Det gir grunn til bekymring at enhver som deltar i organisert idrett kan bli underlagt tilfeldige dopingkontroller. Dette gjelder også brukere av treningssentre, under forutsetning av at de har gitt et forhåndssamtykke. Tilsynet har mottatt klager på at flere treningssentre har gjort dopingtesting obligatorisk for de som ønsker å bli medlem. Testingen vil da ikke være basert på et gyldig samtykke og således være i strid med de vilkår som følger av konsesjonen treningssentre må følge dersom de skal kunne gjennomføre slik testing.

Sikkerhetstiltak rundt fotballkamper

Datatilsynet ble gjort oppmerksom på at personer som kjøper billetter til internasjonale forballkamper blir avkrevd en rekke personopplysninger, herunder fødselsnummer. Opplysningene innhen-

tes for å ivareta sikkerheten rundt arrangementene. Registreringen av opplysninger følger av regelverket til det europeiske forballforbundet (UEFA). I henhold til dette regelverket plikter norske klubber som skal spille bortekamper mot europeiske lag å innhente navn, adresse, passnummer, og dersom det er mulig, også opplysninger om hvor billettkjøperne skal bo under oppholdet i utlandet. Disse opplysningene skal gjøres tilgjengelige for myndighetene i vertslandet og land på reiseruten, samt UEFA-administrasjonen. Det er på det rene at UEFAs regelverk ikke kan sette til side kravene som følger av personopplysningsloven. Datatilsynet har derfor truffet et vedtak som innebærer at norske klubber ikke kan innhente fødselsnummer, og at øvrige personopplysninger kun kan registreres i forbindelse med risikokamper.

Annet

Datatilsynet har også uttalt seg negativt til et nytt verktøy utarbeidet for trenere innenfor lagidretter. Verktøyet innebærer at utøverne utstyres med GPS-sendere som gjør det mulig for trenere å følge den enkeltes bevegelser ned til minste detalj.

Datatilsynet ønsker å innlede et samarbeid med Norges Idrettsforbund for utarbeidelse av retningslinjer for publisering av personopplysninger, herunder bilder, på idrettsforeningers hjemmesider.

9.8 Kameraovervåking

9.8.1 Kameraovervåking i Kristiansand og Trondheim

I 2008 var Datatilsynet på to områdekontroller. Disse fant sted i Nordre gate i Trondheim og i Markens gate i Kristiansand, og omfattet forretninger og virksomheter i handlegatene. Samtlige virksomheter som hadde tatt i bruk kameraovervåking ble gjenstand for kontroll av om virksomheten hadde meldt kameraovervåkingen til Datatilsynet, og om plikten til å merke det kameraovervåkede området var ivaretatt.

Den systematiske gjennomgangen gjør at man akkurat for dette området sitter igjen med god oversikt over overvåkingstetthet, regeletterlevelse og i hvilke bransjer man oftest bruker kameraovervåking.

Overvåkingstettheten i de kontrollerte gatene må samlet sett kunne betegnes som moderat. For Kristiansands del hadde om lag en fjerdedel av virksomhetene tatt i bruk kameraovervåking. Det var omtrent som tilsynet forventet. I Trondheim var andelen lavere enn ventet; om lag en av seks virksomheter hadde tatt i bruk kameraovervåking. Begge områdene hadde lite utendørs overvåking.

Med basis i erfaringer, hadde Datatilsynet forventet en stor andel brudd på melde- og varslingsplikten. Konklusjonen ble imidlertid enda mer nedslående enn antatt. De aller fleste virksomhetene med kameraovervåking unnlot å overholde de enkle og forholdsvis lite byrdefulle pliktene knyttet til overvåkingen. Funnene var forholdsvis like for begge byene. De aller fleste kameraovervåkerne fikk anmerkninger for brudd på meldeplikt og manglende eller ikke tilfredsstillende varsling. Kun én virksomhet, i Kristiansand, fikk ikke anmerkninger for sin kameraovervåking.

Det synes rimelig at en del av forklaringen på at antallet brudd på regelverket er så høyt, er at det har blitt svært enkelt og billig å ta i bruk kameraovervåking. Flere virksomheter later til å tro at det er montørene som skal ivareta lovkravene, mens det i virkeligheten er dem selv som står ansvarlige for at reglene følges.

9.8.2 Overvåking av elever i skoletiden

I meldingsåret så Datatilsynet nærmere på overvåking av skoler i tre kommuner. Kontrollene har vakt stor interesse i media, og har blitt etterfulgt av en rekke henvendelser fra kommuner som ønsker råd i liknede saker.

Den viktigste konklusjonen fra disse kontrollene er at overvåking i skoletiden normalt ikke lar seg rettferdiggjøre. Datatilsynets vurdering er at overvåking i en skolesituasjon må ses som en parallell til overvåking i en arbeidssituasjon. Barn og unge er enda mer sårbare enn voksne, og har i mindre grad forutsetninger for å kunne sette grenser for hva man bør finne seg i. Terskelen for å ta i bruk kameraovervåking i skolen bør derfor ikke være lavere enn på en arbeidsplass, snarere tvert imot.

Kameraovervåking på skolene synes først og fremst å være begrunnet i et ønske om å begrense hærverk. To av de tre kontrollerte kommunene unnlot, eller ønsket å unnlate, å overvåke i skoletiden. Den siste kommunen argumenterte for at de måtte overvåke døgnkontinuerlig.

Etter tilsynets vurdering bør man ikke akseptere en utvikling der barn overvåkes der de oppholder seg, lærer og leker. Skolene har et spesielt ansvar for signalene de sender ut til unge mennesker. Om man godtar en slik utvikling, vil man

raskt kunne få strukturer der barn vokser opp med overvåking, fra og med barnehagen og ut videregående skole. I tillegg til å være et inngrep i barnas personvern, vil en slik utvikling være et langt skritt i retning av en alminneliggjøring av kameraovervåking i samfunnet. Når skoleverket selv bruker slike midler, vil det kunne fungere som en systematisk opplæring av barn og unge til å bli «lydige overvåkingsobjekter», personer som godtar overvåking som en normaltilstand.

9.8.3 Endringer i bruken av kameraovervåking

De kameraovervåkingsanlegg tilsynet i hovedsak ser på kontroller, er forholdsvis tradisjonelle: faste kameraer, koblet til en billedopptaksenhet, gjerne med monitor. Imidlertid har det de siste årene skjedd en overgang fra analog til digital lagring. Lagringen er nå oftere digital enn analog. Digital lagring gjør det enklere å bruke eller kopiere opptak.

Det er vanlig å ha en opptaksenhet som kun gjør opptak når det er bevegelse innenfor det feltet kameraet fanger opp, noe som gjør det enklere å finne tilbake til hendelser.

På noen felter representerer teknologien noe til dels mer inngripende. Overføring av bilder over Internett er en av disse. Når dette skjer på en arbeidsplass, vil sjefen kunne overvåke arbeidsplassen når som helst, og fra hvor som helst, så lenge det er tilgang til Internett.

Datatilsynet har også merket seg at styrbare kameraer med zoomefunksjon ikke er uvanlig. Utstyret gir muligheter for en oppsøkende og nærgående overvåking i langt større grad enn faste kameravinkler og vanlige oversiktsbilder vil kunne gi. Dette fører med seg betydelig større personvernulemper. Datatilsynet mener derfor at denne typen kameraovervåking ikke bør alminneliggjøres.

Økende løsrivelse fra en profesjonell sfære

Kameraovervåking er ikke lenger avgrenset til en profesjonell eller offentlig sfære som i forretninger, banker eller på kjøpesentre.

Datatilsynet mottar forholdsvis mange henvendelser fra privatpersoner som ønsker å igangsette kameraovervåking, for eksempel av egen eiendom og egne verdier. I en del tilfeller er det også andre motiver, som overvåking av leietakere eller naboer. Datatilsynet mottar også mange henvendelser fra privatpersoner som reagerer på andre privatpersoners overvåking. Ofte gjelder disse situasjonene nabokrangler, gjensidig mistillit og beskyldninger. Det synes å være en tendens til at «dummy-kameraer», kameraer som ikke fungerer, er mye i bruk i slike situasjoner, uten at konfliktene blir mindre av den grunn.

Samtidig skjer det også en annen form for løsrivelse fra det «profesjonelle», i form av løsrivelse fra profesjonelle installatører og forhandlere. Det synes å være et større innslag av «gjør-det-selv-løsninger», gjerne basert på bruk av web-kameraer. Dette gjelder både i private sammenhenger, i butikker og på arbeidsplasser. Det eksisterer ofte en svært dårlig konfidensialitetssikring for disse løsningene.

9.9 Samferdsel

Retten til å ferdes fritt anses som en grunnleggende rettighet i et demokrati og er en betingelse for ivaretakelsen av borgernes personvern. For at adgangen til fri ferdsel kan sies å være reell er det ikke tilstrekkelig at man som et utgangspunkt kan reise dit man ønsker, det er en forutsetning at den enkeltes bevegelser ikke registreres, lagres og eventuelt kartlegges. Etter Datatilsynets oppfatning utgjør den økende graden av registrering og lagring av privatpersoners reisemønster en alvorlig trussel mot personvernet.

Samferdselsektoren har samtidig vist seg å være et felt hvor det er vanskelig å få gehør for personvernfremmende tiltak. Datatilsynet har hele tiden hevdet at registrering av den enkeltes bevegelser bare kan aksepteres dersom det er klart nødvendig, for eksempel i forbindelse med fakturering i ettertid. Den behandlingsansvarlig må, som et alternativ, tilby borgeren en anonym reisemulighet.

Elektronisk billettering

Flere kollektivtransportselskaper har innført et elektronisk billettsystem. Løsningene innebærer at den enkeltes reiser registreres og lagres elektronisk. Datatilsynet har i 2008 pålagt Ruter AS å slette reiseopplysninger om passasjerer som benytter klippekort senest tre måneder etter at reisen fant sted. Når det gjelder rene periodebilletter, billetter der man betaler for et ubegrenset antall reiser innen en gitt periode, krever Datatilsynet at lagring av reisemønster må opphøre. Det forutsettes også at transportselskapet tilbyr et likeverdig, anonymt reisealternativ. Vedtaket er påklaget. Personvernnemndas avgjørelse vil bli førende for Datatilsynets vurdering av andre systemer med elektronisk billettering.

Datatilsynet ser med bekymring på at de anonyme alternativene forsvinner, eller gjøres vanskelig tilgjengelig, ved innføring av elektronisk billettering. Omfattende unødvendig lagring av reisehistorikk om den enkelte reisende, samt fravær av sletterutiner for lagrede opplysninger, er et økende problem. Kollektivtransportselskapene gir generelt ikke tilstrekkelig informasjon til de reisende om sin håndtering av personopplysninger, som for eksempel oppbevaring av reisehistorikk.

Automatisk trafikkontroll (ATK) og strekningsvis ATK (SATK)

ATK ble tatt i bruk på begynnelsen av 1990-tallet. Det er fra Samferdselsdepartementets side ønskelig å utvide bruken av slike automatiske kontrolltiltak i veitrafikken. Blant annet vil man ta i bruk såkalt strekningsvis ATK (SATK). I en startfase er det tale om at SATK vil bli tatt i bruk på fem ulike steder i landet. På sikt er det aktuelt å bruke denne kontrollmetoden på rundt 70 strekninger. Datatilsynet reiste tvil om hjemmelgrunnlaget for tiltaket, men Justisdepartementet har i sin tolkning av veitrafikkloven hevdet at lovens § 5 gir tilstrekkelig hjemmel for et slikt tiltak.

Prinsipielt skiller SATK seg fra tradisjonell ATK ved at det blir tatt bilde av samtlige kjøretøy som passerer, ikke bare de som passerer i for høy hastighet. Det blir altså behandlet opplysninger også om fullt lovlydige sjåfører, selv om bildene slettes raskt dersom det viser seg at sjåføren ikke kjører for fort. Igjen vil borgernes bevegelser bli registrert. I et større perspektiv ser dessuten Datatilsynet med bekymring på at stadig mer kontroll av borgernes adferd skjer ved hjelp av automatisk virkende hjelpemidler. Dette er uheldig av flere årsaker. For den enkelte borger vil det være en nærmest håpløs oppgave å tilbakevise opplysninger som er innhentet på dette viset. På sett og vis snus bevisbyrden, påtalemyndigheter kan nøye seg med å vise til «harde fakta», mens den registrerte henvises til å bevise sin uskyld.

Datatilsynet er bekymret for en utvikling der denne infrastrukturen for overvåking tas i bruk til andre formål. Når systemet først ligger der, blir det enkelt å argumentere for at det bør tas i bruk og gjøres tilgjengelig for ulike myndigheter.

Automatiske bomstasjoner og annen bruk av autopass-brikken

Det blir stadig mer utbredt med automatiske bomstasjoner på norske veier. Autopass-systemet, som benyttes til bombetaling i dag, åpner ikke for et reelt anonymt alternativ, for eksempel i form av en ihendehaverbrikke som ikke er knyttet til en person. Dette utgjør en massiv begrensning i bilisters muligheter til fri anonym ferdsel.

Automatiske bomstasjoner er underlagt konsesjonsplikt, og det fremgår av konsesjonsvilkårene at Datatilsynet vil kunne revidere innholdet i konsesjonen. Dette vil bli vurdert fortløpende. Tilsynet ser med bekymring på ulike forslag om å ta autopass-brikken i bruk til stadig nye formål. Det er blant annet fremmet forslag om å innføre en miljøavgift som skal pålegges den faktiske bruken av et kjøretøy. I tillegg til å anvende opplysninger om passering av de eksisterende bomstasjonene, ønsker veimyndighetene å ta i bruk mobile kontrollposter som registrerer passeringer, for eksempel i bykjerner, samt ved kommunegrenser. Dette lovforslaget gikk Datatilsynet sterkt imot. Samtlige kjøretøyer som passerer vil få sin autopassbrikke eller sitt nummerskilt avlest, selv om avgiften kun er tenkt å ramme tunge kjøretøyer. Når kontrollpostene først er etablert, er skrittet videre til utvidet kontroll av stadig flere kjøretøygrupper kort.

9.10 Forskning og helse

9.10.1 Helse

Høring – tilgang til pasientjournaler på tvers av virksomhetsgrenser

I et høringsbrev i meldingsåret la Helse- og omsorgsdepartementet frem forslag til endringer helseregisterloven, helsepersonelloven og forslag til forskrift om informasjonssikkerhet.

Formålet med lovforslagene er å fjerne regelverksmessige hindre for effektiv og trygg kommunikasjon av pasientopplysninger i helsetjenesten.

Etter Datatilsynets vurdering står man i fare for å uthule helsepersonellets taushetsplikt. Ordningen vil medføre at helsepersonell gis adgang til å hente pasientopplysninger i andre helseforetak, uten at det stilles krav om at avgiver i hvert enkelt tilfelle enten vurderer hvorvidt opplysningene er nødvendige og relevante for pasientbehandlingen, eller henter inn samtykke fra pasienten. Dette vil medføre at helsepersonell systematisk kan gis tilgang til overskuddsinformasjon, noe som vil være i strid med gjeldende bestemmelser om taushetsplikt.

Etter tilsynets vurdering kan ikke ordningen fullt ut begrunnes i et dokumentert helsefaglig

behov. Datatilsynet vil peke på at det finnes alternative samhandlingsformer som bedre ivaretar personvernet, og samtidig ivaretar behovet for tilgang til nødvendige og relevante opplysninger ved pasientbehandling. Tilsynet vil særlig peke på elektronisk meldingsutveksling og samtykkebasert kjernejournal.

Datatilsynet reagerer på at Helsedepartementet ikke tar hensyn til de alvorlige mangler ved informasjonssikkerheten som er avdekket ved flere av landets helseforetak. Manglene knytter seg både til dårlig tilgangsstyring for pasientjournaler, og til dårlig kontroll av journallogger der man kan finne opplysninger om hvem som har åpnet hver enkelt pasientjournal. Tilsynet mener at helseforetakene i det minste må få på plass tilfredsstillende, behovsbasert tilgangsstyring internt, før de kan gis anledning til å åpne journalene for ansatte ved andre helseforetak.

Høring: Åstedsundersøkelser ved uventet småbarnsdødsfall

I meldingsåret fremmet Helse- og omsorgsdepartementet et forslag om endringer i *Forskrift om leges melding til politiet*. Det skulle etableres en plikt for leger som gjennomfører dødsstedsundersøkelser ved uventet småbarnsdødsfall (krybbedød) til å melde fra til politiet dersom undersøkelsene avdekket forhold av betydning for fastsetting av dødsårsak, dersom dødsårsaken kan skyldes en straffbar handling.

Ordningen med frivillige dødsstedsundersøkelser er ment å innebære et tilbud til foreldre av barn som dør brått og uventet (krybbedød) om at helsepersonell skal gjennomføre en undersøkelse av dødsstedet, med tanke på å avdekke dødsårsaken. Undersøkelsen skal gjennomføres innen 48 timer.

Datatilsynet reagerte kraftig på at ordningen ble presentert for høringsinstansene som et begrenset unntak fra taushetsplikten. Forslaget innebærer konkret at foreldrene til det døde barnet skal samtykke i etterforskningsliknende tiltak, i de tilfeller hvor det ikke foreligger skjellig grunn til mistanke, og det ikke kan iverksettes ordinær etterforskning. Datatilsynet mener at dette tiltaket ikke kan hjemles i samtykke fra foreldrene. Slike undersøkelser må i dag skje i henhold til straffeprosesslovens bestemmelser. Skal man gjøre unntak fra straffeprosesslovens strenge vilkår om skjellig grunn til mistanke, må også forholdet til EMK artikkel 8 og 6 vurderes. I alle tilfeller må unntaket lovreguleres. Datatilsynet uttalte i sin høringsuttalelse at det var «oppsiktsvekkende at en slik ordning ikke er vurdert i henhold til Grunnlovens § 102 og EMK art 8».

9.10.2 Lov om medisinsk og helsefaglig forskning

Lov om medisinsk og helsefaglig forskning ble vedtatt av Stortinget sommeren 2008, i tråd med odelstingsproposisjonen. Det ble ikke tatt hensyn til de innspill Datatilsynet ga i sin høringsuttalelse og i sin presentasjon til Stortingets helse- og omsorgskomité.

Datatilsynet mener fremdeles at loven er uklar, både i seg selv, og når det gjelder forholdet til omkringliggende regelverk. Det blir problematisk blant annet å fastsette anvendelsesområde, fastslå hvilke krav som skal stilles til sikring av opplysningene, og å avklare de involverte offentlige myndigheters ansvarsområder. Tilsynet har gitt Helse- og omsorgsdepartementet innspill i deres arbeid med å avklare disse og andre spørsmål, og i å utarbeide mer konkrete bestemmelser i forskrifts form. Departementet arbeider frem mot en ikrafttredelse i juli 2009.

Loven vil, når den trer i kraft, få store konsekvenser for Datatilsynets arbeidsoppgaver. Blant annet medfører lovendringen at Datatilsynet ikke skal forhåndsgodkjenne medisinsk og helsefaglig forskning.

Datatilsynet frykter imidlertid at lovendringen også vil medføre et betydelig svekket personvern for pasienter i helsevesenet. Pasientene kan miste kontrollen med bruken av deres biologiske materiale og pasientopplysninger i forskningsøyemed.

9.10.3 Forskning på ulovlig innhentede opplysninger er uetisk

Det såkalte *Hoftebruddsprosjektet* ved Aker Universitetssykehus HF og Universitetet i Oslo, ble stanset med vedtak fra Statens helsetilsyn i 2005. Bakgrunnen var at innsamlingen av det biologiske materialet ble vurdert som uforsvarlig.

Datatilsynet hadde gitt konsesjon til både Hoftebruddsprosjektet og flere tilknyttede delprosjekter. Datatilsynets senere undersøkelser viste at prosjektet også var i strid med personopplysnings- og helseregisterloven. Blant annet forelå brudd på kravet til informert samtykke og i ett tilfelle brudd på konsesjonsplikten. Datatilsynets konsesjoner er gitt under forutsetning av at forskningen skjer i henhold til gjeldende regleverk. Når reglene ikke ble fulgt, mente tilsynet at de tildelte konsesjonene bortfalt som følge av uriktige

forutsetninger. Datatilsynet fattet derfor vedtak om at opplysningene utledet fra prosjektet skulle slettes eller anonymiseres. Universitetet i Oslo og Aker Universitetssykehus HF erklærte senere å ha anonymisert opplysningene.

Datatilsynet ga klart uttrykk for at man fant det svært lite tilfredsstillende at opplysninger som er samlet inn i strid med loven senere blir benyttet i anonymisert form i forskningsøyemed. Fortsatt bruk måtte, etter Datatilsynets mening, i det minste være klarert med de forskningsetiske komiteer.

Universitetet i Oslo la saken frem for Den nasjonale forskningsetiske komité for medisin og helsefag (NEM), som uttalte at de påbegynte PhD- og mastergradene ikke bør ferdigstilles:

> «NEM mener at anonymisering i seg selv ikke kan avhjelpe en situasjon hvor data er innhentet i strid med forskningsetiske prinsipper og rettslige regler. Fordi data er innhentet i strid med forskningsetiske prinsipper, er NEM av den oppfatning at forsøk på å publisere data fra prosjektene kan komme til å skade både stipendiatenes, veilederes og forskningsinstitusjoners omdømme. En publisering av dataene vil også kunne skade den allmenne tilliten til forskningen og forskere, noe både forskningen og befolkningen vil tape på i siste runde.»

9.10.4 Tilsyn i helsesektoren

Støttesystemer for kostnadsfordeling

Datatilsynet kontrollerte våren 2008 to hjelpesystemer innrettet på å fordele kostnader, for henholdsvis transport av pasienter og opphold for gjestepasienter, mellom helseforetakene.

Kontrollen av oppgjørsordningen for gjestepasientopphold ble gjennomført hos Gjestepasientoppgjørskontoret (GOPP) ved Helse Sør-Øst RHF og Rikshospitalet, mens kontrollen av transportordningen ble gjennomført hos *Nasjonalt informasjonssystem for pasienttransport* (NISSY) ved Norsk Helsenett AS og Ullevål Universitetssykehus HF.

For både GOPP og NISSY var det behov for nærmere avklaring av hvordan samarbeid mellom ulike aktører var ordnet:

- Det var til dels uklart hvem som var ansvarlig for de ulike behandlingene av helseopplysningene.
- Nødvendige databehandleravtaler var ikke på plass – noe som for NISSY sin del blant annet skyldtes manglende risikovurderinger av ordningen.
- For GOPP mente Datatilsynet at det var opprettet et ulovlig helseregister i regi av et regionalt helseforetak. For NISSY var det behov for avklaringer med helsemyndighetene før endelige konklusjoner kunne trekkes i forhold til lovligheten av systemet.

Kontrollene med GOPP og NISSY viser tydelig at det er viktig med klare ansvars- og myndighetsforhold. Det regionale helseforetaket påla til dels de enkelte helseforetakene å ta i bruk GOPP og NISSY, samtidig som det reelle ansvaret for at løsningene er i tråd med helseregisterlovens krav ligger hos de enkelte helseforetakene. Slik Datatilsynet ser det tvang det regionale helseforetaket, gjennom sin administrative styringsrett, helseforetakene inn i ulovlig praksis.

Tilgangsstyring innen pleie- og omsorgssektoren

Datatilsynet gjennomførte i 2008 kontroller med fem kommuner med tema tilgangsstyring innen pleie- og omsorgssektoren. Kontrollene viste at det gjenstår en del for å få på plass en tilgangsstyring som i tilstrekkelig grad ivaretar både nødvendig tilgang til tjenestemottakernes journal og beskyttelse mot uautoriserte oppslag – såkalt snoking.

Datatilsynet og Helsetilsynet har delt kompetanse knyttet til kontroll med gitte tilganger og Helsetilsynet deltok derfor som observatør på alle tilsynene.

Det ble sett på hvilke tilganger kommunen hadde gitt i fagsystemene for pleie og omsorg ut i fra tre perspektiver:

- hvor lenge man har tilgang til personopplysninger
- hvor mange personer som har tilgang til opplysningene
- hvor mye informasjon om en person man har tilgang til

Spørsmålet om tilgangsstyring ble løst svært ulikt i kommunene; det én kommune anså som nødvendig, oppfattet andre kommuner som unødvendig. Løsningene ga ikke bare behovsbasert tilgang til journalopplysninger. Som eksempel kan nevnes at alle de ansatte innenfor psykiatri, rus, ergo- og fysioterapi i enkelte tilfeller hadde tilgang til alle pasienter, fordi hvem som helst kunne bli tjenestemottaker hos dem. I ett tilfelle hadde dessuten kjøkkensjefen tilgang til journalopplysninger. De ansatte ble autorisert for tilgang til journalene for

forskjellige tidsrom. Noen kommuner fjernet tilgangsmuligheten når tjenesten opphørte, mens andre tildelte tilgangsrettigheter for all tid fremover. Det var eksempler på at ansatte hadde like stor tilgang til friske, døde og flyttede personer, som til personer som faktisk mottok tjenester.

For at personvernet og taushetsplikten skal ivaretas i de kommunale fagsystemene mener Datatilsynet at systemene må bli mer fleksible. Aktuelle tiltak kan være å la tilgangen avhenge av kjørerute og arbeidsplan, større bruk av midlertidige tilganger og at ansatte ikke får tilgang før de skal behandle tjenestemottakeren. Videre må selve organiseringen av tjenestene understøtte et godt personvern. Det er ikke sikkert at alle sykepleierne på et sykehjem må delta i behandlingen av alle tjenestemottakerne på sykehjemmet.

Datatilsynet kontrollerte om kommunene fulgte opp bruken av de gitte tilgangsrettighetene ved å sjekke loggene. Konklusjonen var at loggingen enten var fraværende, ubrukelig eller at den eksisterte, men ikke ble brukt. Funnene underbygger Datatilsynets skepsis til logging som effektivt middel mot urettmessig tilgang.

Tilgang til helsejournaler ved to sykehus

Datatilsynet kontrollerte i 2008 tilgangen til helsejournaler ved to sykehus.

Ved det første, St. Olavs Hospital HF – Østmarka sykehus, var hovedtemaet for kontrollen tilgangsstyring for pasientopplysninger innen psykiatrien. Kontrollen ble gjennomført med bakgrunn i henvendelser fra ansatte.

Kontrollen avdekket mangler knyttet til pålagt begrensing av tilgang til journal og informasjonssikkerhet, samt internkontroll. Datatilsynet ser funnene som relativt beskrivende for situasjonen i hele sektoren, gitt dagens verktøy og organisering.

Ved den andre kontrollen så Datatilsynet på tilgangen til det fysiske arkivet ved Universitetssykehuset i Nord Norge HF. Kontrollen ble gjennomført som en rask og uanmeldt verifikasjon på bakgrunn av et tips som gjaldt manglende sikring av fysiske pasientjournaler. Datatilsynet fant intet negativt på kontrollen.

9.11 Handel, finans og forsikring

9.11.1 Nasjonalt gjeldsregister

En av de viktigste høringsuttalelsene fra Datatilsynet i 2008 innen finanssektoren, knytter seg til en utredning fra Barne- og likestillingsdepartementet om innføring av et sentralt gjeldsregister. Begrunnelsen for utredningen er at mange privatpersoner opplever økonomiske vanskeligheter på grunn av høy gjeld. Et nasjonalt gjeldsregister vil gjøre det mulig for finansinstitusjonene å undersøke lånekunders eksisterende gjeldsforpliktelser ved vurdering av om et lån skal innvilges eller ikke.

Registeret er ment å inneholde løpende gjeldsforpliktelser for alle myndige nordmenn. Etter det Datatilsynet har erfart anser folk flest private økonomiske opplysninger som svært følsomme opplysninger. Den foreslåtte lovreguleringen innebærer at det ikke vil være frivillig å være registrert i gjeldsregisteret.

Datatilsynet er av den oppfatning at et sentralt gjeldsregister vil være et uforholdsmessig tiltak fordi det vil hjelpe svært få, og samtidig være en personvernulempe for de aller fleste som blir tvunget til å være registrert. Et sentralt gjeldsregister vil heller ikke kunne oppnå en tilfredsstillende opplysningskvalitet. For det første vil flere typer gjeld ikke vil bli registrert, for eksempel privat gjeld og gjeld til utenlandske virksomheter. I tillegg vil det være en tilnærmet umulig oppgave å sikre at registeret til enhver tid er oppdatert.

9.11.2 Høyring – lydopptak av kundar i finansføretak

Føreslåtte endringar i verdipapirføreskrifta opnar for omfattande og unødvendig kontroll av tilsette i finansføretak og deira kundar, skriv Datatilsynet i si høyringsfråsegn. Endringane i føreskrifta inneber mellom anna ei utstrakt plikt for verdipapirføretak til å dokumentere innhaldet i kommunikasjon med sine kundar. I tillegg til krav om lydopptak av telefonsamtalar, skal bruk av SMS, e-post og andre kommunikasjonskanalar i samband med investeringstenester og tilknytta tenester dokumenterast.

I høyringsfråsegna er Datatilsynet også kritiske til om dei føreslegne endringane tener formålet om vern av investorar og auka kontrollmuligheiter.

Datatilsynet er spesielt kritiske til at ei mengd overskotsinformasjon vil bli lagra, noko som kan få store konsekvensar for personvernet. Denne informasjonen vil truleg innehalde personopplysingar av ulik karakter, frå nøytrale til sensitive og følsomme opplysningar. Handsaming av denne typen informasjon er verken sakleg eller relevant, noko som strider mot personopplysingslova.

For tilsette i bankar som driv investeringstenester saman med andre banktenester, medfører

forslaget truleg at det vert gjort opptak av alle inn- og utgåande telefonsamtaler. For dei som nyttar mobiltelefon i både privat- og jobbsamanheng vil dette medføre kontroll av private samtalar. Datatilsynet understrekar at arbeidsgjevar ikkje har sakleg grunn til å føre kontroll med tilsette sin private korrespondanse.

Spørsmål knytt til informasjonsplikt i samband med personopplysingslova er ikkje nemnt i endringsforslaget. Heller ikkje behovet for lagring av opplysningane er nærare omtalt i forslaget.

9.11.3 Ny bankkonsesjon

Banker og finansinstitusjoner må ha konsesjon fra Datatilsynet for å behandle personopplysninger for kundeadministrasjon, fakturering og gjennomføring av banktjenester. Basert på et omfattende tilsynsprosjekt mot 15 banker i 2006, så Datatilsynet et behov for å revidere den nåværende standardkonsesjonen for banker. Særlig var det et behov for å utarbeide klarere vilkår om sletting, tilgangsstyring og kunders rett til innsyn i loggførte oppslag.

Datatilsynet har videre sett et behov for å bygge ut bankkonsesjonen til å omfatte flere formål enn administrasjon av kundeforholdet. Den nye konsesjonen vil også omfatte formålene markedsføring og finansiell rådgivning, risikoklassifisering av kunder og kredittporteføljer, forebygging og avdekking av straffbare handlinger og utvidet lagringstid for kameraovervåking for forebygging og oppklaring av straffbare forhold.

Sparebankforeningen og Finansnæringens hovedorganisasjon har deltatt i jevnlige arbeidsmøter med Datatilsynet i forbindelse med utarbeidelsen av den nye konsesjonen. Det tas sikte på at arbeidet er ferdigstilt i begynnelsen av 2009.

9.11.4 Bransjenorm for inkassobransjen

«Bransjenorm for behandling av personopplysninger i den norske inkassobransjen» ble sluttført våren 2008. Bransjenormen har status som retningslinjer på linje med et internt reglement.

En god bransjenorm er et viktig hjelpemiddel for godt personvern. Normen gir inkassobransjens medlemmer et redskap i arbeidet med å tolke og implementere personvernregelverket, som nok kan oppfattes som omfattende og til dels vanskelig tilgjengelig. I tillegg vil den kunne bidra til at personvernregelverket praktiseres likt innenfor hele bransjen, og vil samtidig være et godt verktøy for de personene som har inkassokrav mot seg.

Brudd på normen kan medføre reaksjoner fra bransjeorganisasjonen. I tillegg vil brudd på normen kunne medføre reaksjoner fra Datatilsynet, i den grad også personopplysningsloven er brutt.

9.11.5 Tilsyn med håndtering av kredittopplysninger

Det gjennomføres stadig flere kredittvurderinger av enkeltpersoner. I 2008 ble det derfor gjennomført tre kontroller hos tilbydere av kredittopplysninger, samt kontroller hos to brukere av kredittopplysninger som blant annet solgte varer på Internett. I følge tall fra tilbyderne av kredittopplysninger, ble det i perioden fra 2005 til 2007 foretatt om lag 20 millioner kredittvurderinger av privatpersoner i Norge.

Saklig behov

For å kunne be om en kredittvurdering må det foreligge et *saklig behov* for dette. Saklig behov kan for eksempel foreligge ved kredittkjøp eller ved forespørsler om lån. Den som innhenter kredittvurderinger skal ikke skaffe seg flere opplysninger enn det er behov for. Det kan kun lagres informasjon om at kredittsjekken er gjennomført. Selve innholdet skal slettes.

Tilsynene viste at kredittvurderinger i hovedsak ble foretatt online av virksomheter som kjøpte kredittopplysninger, og det var opp til den som søkte etter kredittopplysninger å vurdere om saklighetskravet var oppfylt. Avtalene som kredittopplysningsbyråene inngikk med sine abonnenter ga ingen eller liten veiledning om hva saklighetskravet innebærer. Tilsynene hos brukerne av kredittopplysninger viste at man også gjennomførte kredittvurderinger ved marginale kjøp, hvor et kredittelementet knapt kan sies å foreligge, samt for å sile ut de kundene man ikke ønsket å handle med.

Det skal ikke innhentes flere opplysninger enn det som er nødvendig. I enkelte tilfeller vil det for eksempel være tilstrekkelig kun å innhente opplysninger om betalingsmislighold. Selv om enkelte av løsningene til kredittopplysningsbyråene åpnet for å begrense mengden av opplysninger som skulle innhentes, viste én av kontrollene at denne muligheten ikke ble benyttet. Det var enklere å innhente alle opplysningene som kredittopplysningsbyrået hadde om en person, enn å spesifisere hvilke opplysninger en ønsket.

Virksomhetene som abonnerte på tilgang til kredittopplysninger lagret, med få unntak, ikke

selve kredittvurderingen (som for eksempel opplysninger om inntekt, formue og betalingsmislighold). At kreditt var blitt nektet ble imidlertid aldri slettet, unntatt i de tilfellene der kredittvurderingen skjedde automatisk ved bestilling på Internett.

Gjenpartsbrev

Ved innhenting av kredittvurderinger skal det sendes et gjenpartsbrev til vedkommende som blir vurdert. Brevet skal informere om hvem som har innhentet vurderingen, samt angi hvilke opplysninger som er blitt utlevert.

Ett av produktene som kan innhentes fra kredittopplysingsbyråene er en *score*. Scoren angir statistisk sannsynlighet for betalingsmislighold for en bestemt person eller virksomhet. Gjenpartsbrevene inneholdt aldri opplysinger om scoren. Datatilsynet har pålagt kredittopplysningsbyråene å opplyse om dette. Byråene har påklaget dette til Personvernnemnda.

Byråene brukte tidligere navn og adresser i scoren. Datatilsynet har uavhengig av kontrollene pålagt byråene å slutte med å bruke disse opplysningene i scoren. Saken ble påklagd til Personvernnemnda som har gitt Datatilsynet medhold.

Ikke rutiner for å avdekke misbruk internt i kredittopplysningsbyråene

Ingen av byråene hadde utarbeidet rutiner for å undersøke om ansatte misbrukte muligheten for å foreta kredittvurderinger der gjenpartsbrev ikke ble sendt. Enkelte ansatte i kredittopplysningsbyråene kunne få tilgang til kredittopplysningsdatabasen fra en hvilken som helst pc med internettilgang, uten at gjenpartsbrev ble sendt.

9.11.6 Direkte markedsføring – overføring av bestemmelsene til markedsføringsloven

Reglene om direkte markedsføring og reservasjonsregisteret skal flyttes fra personopplysningsloven til markedsføringsloven 1. juni 2009. Datatilsynet har deltatt i arbeidsgrupper i regi av Barne- og likestillingsdepartementet i den forbindelse.

Datatilsynet var positivt til forslaget i sin høringsuttalelse. I dag finnes reglene for direktemarkedsføring både i markedsføringsloven og personopplysningsloven, som forvaltes av henholdsvis Forbrukerombudet og Datatilsynet. En slik løsning er uoversiktlig både for markedsføreren, myndighetene og ikke minst for forbrukeren.

Vedlegg 1:

Tilsynsobjekter

Sektor	Antall	Sak	Omtale
Kommune	1	08/00231	Kontroll hos Bø kommune 27032008 – ACOS AS – Offentlig nettside
Kommune	1	08/00232	Kontroll hos Bærum Kommune 26022008 – KF Skjema
Databehandler	1	08/00238	Kontroll ved Kommuneforlaget 26022008 – KF Skjema
Databehandler	1	08/00239	Kontroll hos ACOS AS 21022008
Kommune	1	08/00250	Kontroll hos Fredrikstad Kommune 28032008
Kommune	1	08/00251	Kontroll hos Molde kommune 01042008 – KF Skjema
Kommune	1	08/00252	Kontroll hos Elverum Kommune 06032008 – KF Skjema
Kommune	1	08/00254	Kontroll hos Stange Kommune 07032008
Elektronisk kommunikasjon	1	08/00255	Kontroll hos Lyse Energi AS i Stavanger 12032008 – Tilbydere av e-post tjenester
Elektronisk kommunikasjon	1	08/00256	Kontroll hos Direct Connect 14032008
Elektronisk kommunikasjon	1	08/00258	Kontroll hos comm.age as 03042008 – Tilbydere av e-post tjenester
Advokat	1	08/00275	Kontroll hos Brækhus Dege Advokatfirma ANS 27052008 – Elektronisk kommunikasjon
Innkrevning	1	08/00283	Kontroll hos Statens Innkrevingssentral 06052008
Stat	1	08/00291	Kontroll hos Altinn sentralforvaltning og Altinn-portalen 14052008 – Brønnøysundregistrene
Stat	1	08/00297	Kontroll hos Skattedirektoratet 14052008 – Altinn Sentralforvaltning
Elektronisk kommunikasjon	1	08/00301	Kontroll hos Carrot Communications ASA 29042008 – Telekommunikasjon
Elektronisk kommunikasjon	1	08/00302	Kontroll hos Eurobate AS 23042008 – Telekommunikasjon
Kommune	1	08/00306	Kontroll hos Tromsø kommune / Kvaløysletta sykehjem 03032008 – tilgang til helseopplysninger – Pleie- og omsorg
Kommune	1	08/00307	Kontroll hos Sarpsborg kommune 06032008 – tilgang til helseopplysninger – Pleie- og omsorg
Kommune	1	08/00308	Kontroll hos Ørskog kommune 07032008 – tilgang til helseopplysninger – Pleie- og omsorg
Kommune	1	08/00309	Kontroll hos Orkdal kommune 25032008 – tilgang til helseopplysninger – Pleie- og omsorg
Kommune	1	08/00310	Kontroll hos Dovre kommune/Fredheim omsorgssenter 28032008 – Pleie- og omsorg
Helse	1	08/00312	Kontroll hos Norsk Helsenett 26032008 – NISSY
Helse	1	08/00313	Kontroll hos Ullevål universitetssykehus HF 03042008 – NISSY
Helse	1	08/00314	Kontroll hos Universitetssykehuset i Nord Norge HF 03032008 – Papirjournalarkiv

Sektor	Antall	Sak	Omtale
Helse	1	08/00315	Kontroll hos St Olavs Hospital HF Østmarka sykehus 27032008 – Tilgang til helseopplysninger i elektroniske journalsystemer
Kamera	1	08/00319	Kontroll hos Jernbaneverket – Eidsvoll stasjon 11042008 – kameraovervåking
Justis	1	08/00325	Kontroll hos Oslo politikammers personalbarnehage Egon barnehage 14022008 – Oslo politidistrikt – med tilgang til personopplysninger
Kamera	1	08/00334	Kontroll hos Radisson SAS Scandinavia Hotel Holbergsplass – kameraovervåking
Nummeropplysning	1	08/00336	Kontroll hos Lindorff Match 14042008
Kredittopplysning	1	08/00337	Kontroll hos Dun & Bradstreet 10042008 – Kredittopplysningsvirksomhet
Kredittopplysning	1	08/00338	Kontroll hos Lindorff Decision AS 14042008 – Kredittopplysningsvirksomhet
Kredittopplysning	1	08/00339	Kontroll hos Creditinform AS 11042008 – Kredittopplysningsvirksomhet
Kredittopplysning	0	08/00340	Kontroll hos IKEA AS 07042008 – Kredittopplysningsvirksomhet
Kredittopplysning	1	08/00341	Kontroll hos Samlerhuset AS 08042008 – Kredittopplysningsvirksomhet
Arbeidsliv	1	08/00342	Kontroll hos Stavanger kommune 15042008
Kamera	1	08/00346	Kontroll hos Harveys Tronheim AS – 12032008 – kameraovervåking
Kamera	1	08/00348	Kontroll ved Lerkendal Stadion 12032008 – kameraovervåking
Elektronisk kommunikasjon	1	08/00350	Kontroll hos Combitel / MTU Nett 26032008 – Tilbydere av e-post tjenester
Kamera	1	08/00351	Kontroll hos Stiftelsen Trondheim Pirbad 11032008 – kameraovervåking
Kamera	1	08/00353	Kontroll hos Bærum kommune 26032008 – Kameraovervåking ved Nadderudhallen
Advokat	1	08/00355	Kontroll hos Advokatfirmaet Hestenes og Dramer & Co ANS 15042008 – elektronisk kommunikasjon
Advokat	1	08/00356	Kontroll hos Advokatfirmaet Strand & Co ANS 17042008 – Elektronisk kommunikasjon
Advokat	1	08/00357	Kontroll hos Advokathuset Trondheim DA 18042008
Kamera	1	08/00358	Uanmeldt kontroll hos Åslundmarka legesenter 02042008 – Kameraovervåking
Helse	0	08/00359	Kontroll med Helse Sør-Øst RHF 05032008 – Bruk av NISSY
Justis	1	08/00361	Kontroll hos Politidirektoratet 02042008 – førerkortregisteret – prikkbelastningssystemet
Justis	1	08/00363	Kontroll hos Politidirektoratet 01042008 – våpenregisteret
Justis	1	08/00366	Kontroll hos Politidirektoratet 03042008 – passregisteret
Elektronisk kommunikasjon	1	08/00394	Kontroll hos Chess Communication AS 27032008
Elektronisk kommunikasjon	1	08/00395	Kontroll hos One Call AS 08042008 – Tilbydere av e-post tjenester

Sektor	Antall	Sak	Omtale
Elektronisk kommunikasjon	1	08/00396	Kontroll hos Start Network AS 10042008 – Tilbydere av e-post tjenester
Elektronisk kommunikasjon	1	08/00397	Kontroll hos Tele2 Norge AS 15042008
Biometri	1	08/00398	Kontroll hos SAS Norge 11042008 – Bruk av reisendes fingeravtrykk – Biometri
Biometri	1	08/00400	Kontroll hos DnB NOR Bank avdeling Homansbyen i Hegdehaugsveien 25032008 – Biometri
Kredittopplysning	1	08/00410	Kontroll hos Webzoo AS 07042008 – Kredittopplysningsvirksomhet
Forsikring	1	08/00411	Kontroll hos IF Skadeforsikring/Falck 12032008 – sporingsenhet i bil – If tracker
Kamera	1	08/00413	Kontroll hos Horten kommune 16052008 – kameraovervåking i regi av kommunen
Kamera	1	08/00414	Kontroll hos Nøtterøy kommune 15052008 – kameraovervåking i regi av kommunen
Kamera	1	08/00416	Kontroll hos Rogaland Teater 16042008 – Lyd- og billedoverføring
Kamera	1	08/00418	Kontroll hos Lørenskog kommune 17042008 – kameraovervåking i kommunens regi
Innkrevning	1	08/00420	Kontroll hos Forsvaret 04042008 – Forsvarets bruk av Statens Innkrevningssentral
Forsvaret	1	08/00430	Kontroll hos Forsvaret 28032008 – Vernepliktsverket Lillehammer – Behandling av personopplysninger fra sesjon og førstegangstjeneste
Stat	3	08/00436	Kontroll ved norske utenriksstasjoner – Ambassadene – Moskva 08052008 – London 23052008 og Ankara 11062008 – Utenriksdepartementet
Stat	1	08/00439	Kontroll hos Husbanken 16042008 – Behandling av personopplysninger ifm løsningen Bokart
Justis	1	08/00443	Kontroll hos Drammen politistasjon/Søndre Buskerud politidistrikt 17042008 – Kameraovervåking
Justis	1	08/00444	Kontroll hos Tønsberg politistasjon/Vestfold politidistrikt 17042008
Biometri	1	08/00445	Kontroll hos Munch museet 23042008 – Adgangskontrollsystem
Kamera	1	08/00450	Kontroll hos Teletopia 25022008
Forsvaret	1	08/00452	Kontroll hos Forsvaret 23042008 – Forsvarets Mediesenter – Innsamling av personopplysninger over Internett
Forskning	1	08/00543	Kontroll med Nasjonalt hoftebruddsregister 27032008 – Helse Bergen HF
Kamera	1	08/00574	Kontroll – Områdekontroll av kameraovervåking i Trondheim 12032008 – MIX Byhaven
Kamera	1	08/00575	Kontroll – Områdekontroll av kameraovervåking i Trondheim 12032008 – Cafe Orange
Kamera	1	08/00576	Kontroll – Områdekontroll av kameraovervåking i Trondheim 12032008 – Narvesen 347
Kamera	1	08/00577	Kontroll – Områdekontroll av kameraovervåking i Trondheim 12032008 – Ark Bruns
Kamera	1	08/00578	Kontroll hos 7-Eleven Thomas Angell 12032008 – Områdekontroll av kameraovervåking i Trondheim

Sektor	Antall	Sak	Omtale
Kamera	1	08/00579	Kontroll – Områdekontroll av kameraovervåking i Trondheim12032008 – Carma
Kamera	1	08/00580	Kontroll – Områdekontroll av kameraovervåking i Trondheim – Ole Aas AS
Kamera	1	08/00581	Kontroll hos Restauranthuset Carl Johan AS/ Vertshuset chevalier 12032008 – Områdekontroll av kameraovervåking i Trondheim
Helse	1	08/00907	Kontroll hos Nasjonalt kunnskapssenter for helsetjenesten 1606208 – FS-systemet
Helse	1	08/00969	Kontroll hos Rikshospitalet HF 03062008 – GOPP – Gjestepasientoppgjørskontoret
Kamera	1	08/01059	Kontroll av kameraovervåking i boligstrøk – Stavanger 15042008
Kamera	1	08/01107	Kontroll ved Øvre Haukeligate 24 15042008 – Kameraovervåking
Kamera	1	08/01152	Uanmeldt kontroll hos Thinh lunsjbar på Aker Brygge i Oslo 25062008
Kundeopplysninger	1	08/01440	Kontroll hos Hjemmet Mortensen AS – 06102008
Samferdsel	1	08/01441	Kontroll hos Tollpost Globe AS – 28112008 – Flåtestyringsverktøy
Samferdsel	1	08/01442	Kontroll hos Schenker AS 26112008 – Bruk av flåtestyringsverktøy
Samferdsel	0	08/01443	Kontroll hos Coca- Cola Norge AS 19112008 – Bruk av flåtestyringsverktøy
Varsling	1	08/01444	Kontroll hos Universitetet for miljø- og biovitenskap – 10102008 – Varslingsrutiner
Helse	0	08/01445	Kontroll hos Hjelp 24 Bedriftshelsetjeneste – 21102008 – Bedriftshelsetjeneste
Helse	1	08/01446	Kontroll hos Brynklinikken Bedriftshelsetjeneste – 27102008 – Bedriftshelsetjenester
Helse	1	08/01447	Kontroll hos Oslo City Legesenter – 07102008 – Bedriftshelsetjenester
Helse	1	08/01448	Kontroll hos Rikshospitalet Bedriftshelsetjeneste – 30102008 – Bedriftshelsetjenester
Finans	1	08/01449	Kontroll hos Dolly Dimple's / PAM AS – 11112008 – Kredittkortinformasjon
Finans	1	08/01450	Kontroll hos Pizza og Kinaekspressen – 06112008 – Kredittkortinformasjon
Finans	1	08/01451	Kontroll hos Spice AS – 04112008 – Kredittkortinformasjon
Helse	1	08/01452	Kontroll hos MEDI 3 Sjølyst AS (tidligere Sjølyst Medisinske senter AS) – 09102008 – Bedriftshelsetjeneste
Varsling	1	08/01453	Kontroll hos Oslo Kommune – Byrådlederens avdeling 09102008 – Varslingsrutiner
Identitetsforvaltning	1	08/01454	Kontroll hos Oberthur Technologies Norsik AS 07102008 – ID kort i byggebransjen
Personprofil	1	08/01455	Kontroll hos Assessio Assignment AS – 04112008 – Personlighetstester
Varsling	1	08/01456	Kontroll hos Universitetet i Bergen – 16102008 – Varslingsrutiner

Sektor	Antall	Sak	Omtale
Varsling	1	08/01457	Kontroll hos Hordaland fylkeskommune – 17102008 – Varslingsrutiner
Varsling	1	08/01458	Kontroll hos Oppland fylkeskommune – 21102008 – Varslingsrutiner
Varsling	0	08/01459	Kontroll hos Norsk Hydro 29102008 – Varslingsrutiner
Personprofil	1	08/01460	Kontroll hos PA Consulting Group AS – 07112008 – Personlighetstester
Personprofil	1	08/01461	Kontroll hos Scientologikirken Oslo – 21112008 – Personlighetstester
Utdanning	1	08/01497	Kontroll hos Akershus fylkeskommune – 11112008 – Bruk av læringsplattform – Læringsplattform
Utdanning	1	08/01498	Kontroll ved Drømtorp videregående skole 18112008 – Akershus fylkeskommune – Elev PC
Utdanning	1	08/01499	Kontroll hos Hedmark fylkeskommune 28102008 – Bruk av læringsplattform
Utdanning	1	08/01500	Kontroll ved Storhamar videregående skole 28102008 – Hedmark fylkeskommune – Bruk av læringsplattformer
Utdanning	1	08/01501	Kontroll ved Sandvika videregående skole 14102008 – Akershus fylkeskommune – Bruk av læringsplattform
Utdanning	1	08/01502	Kontroll ved Lillestrøm videregående skole 16102008 – Akershus fylkeskommune – Bruk av læringsplattform
Utdanning	1	08/01505	Kontroll ved Eiker videregående skole 13112008 – Buskerud fylkeskommune – Elev PC
Krisesenter	1	08/01509	Kontroll hos Stiftinga krisesenteret i Sogn og Fjordane – 29102008 – Krisesenter
Krisesenter	1	08/01510	Kontroll hos Betzy krisesenter – 03112008 – Krisesenter
Krisesenter	1	08/01511	Kontroll hos Kongsberg krisesenter – 03112008 – Krisesenter
Krisesenter	1	08/01512	Kontroll hos Krisesenteret i Telemark – 04112008 – Krisesenter
Krisesenter	1	08/01513	Kontroll hos Stiftelsen Krisesenteret for kvinner i Vestfold – 04112008 – Krisesenter
Utlendingsforvaltning	1	08/01514	Kontroll hos Bergum asylmottak i Førde – Hero Norge AS og UDI – 28102008 – Asylmottak
Utlendingsforvaltning	2	08/01518	Kontroll hos Tanum transittmottak 27102008 – Norsk Folkehjelp og UDI – Asylmottak
Utlendingsforvaltning	1	08/01526	Kontroll hos Utlendingsdirektoratet 15102008 og Politiets utlendingsenhet 17102008 – Utlendingsforvaltningen
Utlendingsforvaltning	1	08/01528	Kontroll hos Kripos – Dokumentasjonskontroll med frist 10102008
Utlendingsforvaltning	1	08/01556	Granskning hos Skattedirektoratet 10102008 – Uautorisert utlevering av personopplysninger
Utlendingsforvaltning	1	08/01567	Kontroll med Eurodac – Utlendingsdirektoratet 061008 og 171008 – Utlendingsforvaltningen

Sektor	Antall	Sak	Omtale
Helse	1	08/01617	Kontroll hos Bedriftshelsetjenesten Helse & Jobb – 21102008 – Bedriftshelsetjeneste
Helse	0	08/01649	Kontroll hos Akershus Universitetssykehus HF 16102008
Kamera	1	08/01709	Uanmeldt kontroll hos Esthetique 23102008 – Kameraovervåking
Kamera	1	08/01710	Uanmeldt kontroll hos Elite Foto Wintersborg Kristiansand as 23102008 – Kameraovervåking
Kamera	1	08/01711	Uanmeldt kontroll hos Vero Moda i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01713	Uanmeldt kontroll hos Markens Godteri og isbar 23102008 – Kameraovervåking
Kamera	1	08/01714	Uanmeldt kontroll hos Narvesen 421 i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01716	Uanmeldt kontroll hos Hodne og Wroldsen i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01717	Uanmeldt kontroll hos Juvelen i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01718	Uanmeldt kontroll hos Cubus i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01719	Uanmeldt kontroll hos 7 eleven i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01720	Uanmeldt kontroll hos Mc Donald – Hots Invest AS i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01735	Uanmeldt kontroll hos Change i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01736	Uanmeldt kontroll hos Esthetique i Markensgate i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01737	Uanmeldt kontroll hos Megastore i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01738	Uanmeldt kontroll hos Sparebanken Pluss i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01739	Uanmeldt kontroll hos Buksesmekken i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01740	Uanmeldt kontroll hos Nordea i Markensgate i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01741	Uanmeldt kontroll hos Sparebank1 – SR bank i Kristiansand 23102008 – Kameraovervåking
Kamera	1	08/01752	Uanmeldt kontroll hos Narvesen – Markensgate Kristiansand 23102008 – Kameraovervåking
Kamera	0	08/01997	Områdekontroll Kristiansand – Kamera
Sum	141		

Vedlegg 2

Personvernnemndas årsmelding 2008

1 Sammendrag

Dette er Personvernnemndas åttende årsmelding. I løpet av året er det kommet seks klager, alle er ferdigbehandlet i 2008. Dessuten er tre klager fra 2007 ferdigbehandlet. I alt er det altså ferdigstilt ni klagesaker i løpet av året. Datatilsynets vedtak er omgjort helt eller delvis i tre av de ni sakene.

Saksmengden har vært stabil i forhold til 2007, hvor det ble behandlet totalt 11 saker. Personvernnemnda antar at saksmengden nå vil stabilisere seg på ca 10-12 klagesaker i året.

Flere av sakene har vært komplekse og prinsipielle. Personvernnemnda kan bare ta stilling i konkrete saker, men ser at det på flere områder er behov for en sektorovergripende rettspolitisk debatt. Nemnda er derfor glad for at Personvernkommisjonen ble opprettet. Et av varamedlemmene i nemnda – Mari Bø Haugstad – har også vært medlem av Personvernkommisjonen i 2008.

2 Innledning

Personvernnemnda er opprettet med hjemmel i lov om behandling av personopplysninger (2000:31). Loven trådte i kraft 1.1.2001. Personvernnemnda er et klageorgan for vedtak fattet av Datatilsynet etter personopplysningsloven og etter helseregisterloven (2001:24).

Personvernnemnda er et uavhengig forvaltningsorgan administrativt underlagt Kongen og Fornyings- og administrasjonsdepartementet (FAD).

Personvernnemndas arbeid reguleres av personopplysningsloven, forskrifter til denne, samt en instruks som departementet har utarbeidet. Forvaltningsloven og offentlighetsloven kommer også til anvendelse som for forvaltningen for øvrig.

Selv om departementet utarbeider instruks, innebærer dette ikke noen form for instruksjonsmyndighet i enkeltsaker. Departementet kan ikke gi generelle instrukser om lovtolkning eller skjønnsutøvelse.

Personvernnemnda skal årlig orientere Kongen om behandling av klagesakene.

3 Medlemmer

Personvernnemnda har syv medlemmer som blir oppnevnt for fire år med adgang til oppnevning for ytterligere fire år. Personvernnemndas leder og nestleder oppnevnes av Stortinget, mens de øvrige medlemmer oppnevnes av Kongen. Første gangs oppnevning skjedde i 2001. I 2005 ble leder og nestleder, samt medlemmene Siv Bergit Pedersen og Hanne Inger Bjurstrøm, oppnevnt for fire nye år. Disse fire har i 2008 hatt sitt siste år av funksjonstiden i nemnda. Det ble også oppnevnt tre nye medlemmer i 2005, som i desember 2008 ble gjenoppnevnt for fire nye år. I desember 2008 ble det også oppnevnt ny leder og nestleder, samt to nye medlemmer, som starter sin funksjonstid 1.1.2009.

Personvernnemnda besto i 2008 av følgende personer:

- Jon Bing, leder
- Gro Hillestad Thune, nestleder
- Siv Bergit Pedersen
- Hanne I Bjurstrøm
- Tom Bolstad
- Leikny Øgrim
- Jostein Halgunset

I tillegg har alle medlemmene personlige vararepresentanter.

4 Andre organisatoriske forhold

Sekretariatet til Personvernnemnda består av Tonje Røste Gulliksen, som ble ansatt som seniorrådgiver i Fornyingsdepartementet i 2005. Sekretariatet er samlokalisert med Forbrukerrådet og Forbrukerombudet i Rolf Wickstrøms vei 15 i Nydalen. Sekretæren avvikler såkalt gradert uttak av fødselspermisjon. Dette har ikke skapt praktiske problemer for nemndas arbeid.

Personvernnemnda holder sine møter i lokaler utenfor Datatilsynet og Regjeringskvartalet for også på denne måten å markere uavhengighet.

Personvernnemnda har egen hjemmeside, *www.personvernnemnda.no*, hvor blant annet vedta-

kene er publisert i sin helhet. Hjemmesiden har lenke fra Datatilsynets hjemmeside, og lenker til personvernrelatert materiale tilgjengelig på Internettet. Personvernnemndas vedtak publiseres også i en egen database hos Lovdata lenket til det øvrige dokumenterte materialet. Dermed kan en bruker lett slå opp på Personvernnemndas vedtak ved oppslag på paragraf i personopplysningsloven, andre lover, dommer mv. som vedtakene viser til.

5 Møter og konferanser 2008

Personvernnemnda har i 2008 hatt i alt ni møter. Møtene ble i hovedsak nyttet til å behandle klagesaker, men også administrative forhold har blitt behandlet.

I tillegg til nemndmøter har det vært forberedende møter med sekretariatet og leder.

Personvernnemnda hadde to kontaktmøter med departementet i 2008, i juni og november.

Personvernnemnda deltok på den internasjonale konferansen for datatilsynsmyndigheter i Strasbourg, Frankrike, 15. – 17. oktober. Leder Jon Bing, nestleder Gro Hillestad Thune og sekretær Tonje Røste Gulliksen representerte nemnda.

Personvernnemnda ytet økonomisk støtte til «Personvernkonferansen 2008», som ble arrangert av Avdeling for forvaltningsinformatikk, Universitetet i Oslo, 5.12.2008. Flere av Personvernnemndas medlemmer deltok på konferansen. Tema for konferansen var «Personvern – også i skolen?». Konferansen belyste personvern for barn og ungdom og drøftet personvern i skolen over en bred front. Konferansen var fulltegnet.

6 Evaluering av nemndas arbeid 2001–2008

Personvernnemnda inngikk i september 2008 en avtale med professor ved Københavns Universitet, Peter Blume, som er en anerkjent personvernrettsekspert. Blume er også medlem av Datarådet i det danske datatilsynet.

Bakgrunnen for avtalen var at nemnda snart skulle avslutte sin andre funksjonsperiode ved utgangen av 2008. Nemnda ønsket derfor en uavhengig, overordnet gjennomgang og vurdering av de vedtak som nemnda har truffet, med vekt på typer av vurderinger som nemnda har foretatt, Personvernnemndas praksis i forhold til den internasjonale utvikling og hvordan nemndas skjønn henger sammen med retninger og trender i andre europeiske land.

På bakgrunn av sin gjennomgang av Personvernnemndas praksis holdt Blume et innlegg under den årlige personvernkonferansen 5. desember. Han leverte sin rapport til nemnda 22. desember. Rapporten er publisert på Personvernnemndas hjemmeside.

7 Klagesaksbehandling

Personvernnemnda mottok i 2008 totalt seks klagesaker. Samtlige av disse var ferdigbehandlet ved utgangen av året. I tillegg ble tre saker fra 2007 ferdigbehandlet i 2008. Oversikt over vedtakene, samt vedtakene i sin helhet, er publisert på Personvernnemndas hjemmesider. I tillegg er vedtakene publisert i egen database hos Lovdata.

Saksmengden har holdt seg stabil i forhold til 2007. Flere av sakene har vært prinsipielle.

Personvernnemnda vil særlig fremheve to forhold i årsmeldingen.

Det første forholdet gjelder sakene om kredittopplysningsbransjen, PVN-2008-04 Lindorff og PVN-2008-05 Creditinform. Datatilsynet har laget en standardkonsesjon for kredittopplysningsforetak. Bruk av standardkonsesjon er et enkeltvedtak, men det binder Datatilsynet opp i å benytte samme konsesjon for alle foretak innen bransjen uten at dette har vært gjenstand for høring o.a. Etter nemndas syn ville det være mer hensiktsmessig å lage en forskrift med de rettssikkerhetsgarantier det medfører.

Det andre forholdet gjelder saken om det sentrale straffe- og politiopplysningsregisteret, PVN-2008-02 SSP. I denne saken mener nemnda at det er grunn til rettspolitisk ettertanke. Nemnda etterlyser en generell og overordnet rettspolitisk diskusjon av politiets registrering, oppbevaring, bruk og sletting av sensitive opplysninger. Etter nemndas syn bør det oppmuntres til en debatt blant relevante parter om hvordan dette systemet bør bygges opp. I en slik vurdering er det politifaglige bare et aspekt. Det andre aspektet gjelder datalagring og datasanering generelt. Dette er et prinsipielt spørsmål som berører nærmest alle sektorer og er et viktig samfunnsspørsmål.

Saker som ble behandlet i 2008 er:

PVN-2007-02 Bibliotek-Systemer

Klage på Datatilsynets avslag hvoretter Bibliotek-Systemer AS ikke får utvikle bibliotektjeneste som inne-

bærer å lage knytninger mellom boktitler som ulike låntakerne låner – såkalt korrelasjonsdatabase

Bibliotek-Systemer AS har påklaget et vedtak fra Datatilsynet som går ut på at de ikke får utvikle en bibliotektjeneste som innebærer å lage knytninger mellom boktitler som ulike boklåntakerne låner – en såkalt korrelasjonsdatabase. Datatilsynet er av den oppfatning at tjenesten innebærer en personverntrussel. Det vises til at det opprinnelige formålet med bibliotekenes låneopplysninger er å administrere låneforholdet. Som en følge av dette skal opplysningene normalt slettes når boken leveres tilbake, jf personopplysningsloven § 28. Nemnda mener at personverntrusselen er liten, men kommer likevel til at Bibliotek-Systemer AS kun har adgang til å etablere en korrelasjonsdatabase dersom det innhentes samtykke fra de registrerte.

PVN-2007-06 OBOS

Klage på Datatilsynets avvisningsvedtak. Begjæring om innsyn i dokumenter, advokaters taushetsplikt og spørsmål om hvor langt Datatilsynets utredningsplikt går

Klager begjærte innsyn i opplysninger i forbindelse med en konflikt mellom et OBOS-borettslag og klagers mor, jf personopplysningsloven § 18. Datatilsynet fulgte opp innsynsbegjæringen, men avsluttet saken da OBOS påberopte at innsyn ikke kunne gis fordi opplysningene er unntatt fra innsynsretten etter personopplysningsloven § 23 litra d, med bakgrunn i advokaters taushets- og konfidensialitetsplikt, jf domstolloven § 224 og advokatforskriftens kap 12 pkt 2.3. Nemnda tok ikke klagen til følge. Datatilsynet hadde oppfylt sin utredningsplikt etter forvaltningsloven. Det var ikke en saksbehandlingsfeil at Datatilsynet ikke gjennomførte en stedig kontroll hos OBOS i denne saken.

PVN-2007-07 ung1881.no

Klage på Datatilsynets vedtak om at Opplysningen må innhente samtykke fra abonnent før Opplysningen kan benytte informasjon om brukere av mobiltelefonnummer som de får på nettstedet ung1881.no til å oppdatere sin opplysningstjeneste

Klage på Datatilsynets vedtak om at Opplysningen må innhente samtykke fra abonnent før Opplysningen kan benytte informasjon om brukere av mobiltelefonnummer som de får på nettstedet ung1881.no til å oppdatere sin nummeropplysningstjeneste. Nemnda tok ikke klagen til følge og viste til at dette er regulert i ekomforskriften § 6-3. Ekomforskriften gir abonnenten kontroll med hvilke opplysninger som gjøres tilgjengelig for allmennheten, og det bryter mot denne ordningen at man åpner en «bakvei» for uavhengig av abonnenten å endre eller supplere opplysningene. Nemndas flertall kom til at Opplysningen må be om samtykke fra abonnenten før informasjonen fra ung1881.no kan brukes til å oppdatere nummeropplysningstjenesten, jf hovedregelen i personopplysningsloven § 8.

PVN-2008-01 Utleiemegleren

Klage på Datatilsynets vedtak om at Utleiemegleren skal stanse sin behandling av kredittopplysninger vedrørende interessenter til leie av boliger

Klage på Datatilsynets vedtak om at Utleiemegleren skal stanse sin behandling av kredittopplysninger vedrørende interessenter til leie av boliger. Datatilsynet mente at Utleiemegleren ikke har et «saklig behov» for å innhente kredittopplysninger om interessenter, jf personopplysningsforskriften § 4-3. Datatilsynet viste til flertallets vurderinger i KLP-saken, PVN-2006-03. Personvernnemnda kom etter en konkret vurdering kommet til at det i denne saken foreligger saklig behov for kredittopplysninger. Saken skiller seg fra KLP-saken fordi Utleiemegleren handler på vegne av enkeltpersoner. For en privatperson er det en høy forretningsmessig risiko forbundet med boligutleie. Nemnda mener at kun den som får tilbud om å leie boligen kan bli kredittvurdert som en siste sjekk før tilbudet gis.

PVN-2008-02 SSP

Klage på Datatilsynets vedtak om at Kripos skal slette opplysninger om en person i det sentrale straffe- og politiopplysningsregisteret (SSP)

Personvernnemnda kom til at domstolens beslutning om varetekt faller innenfor personopplysningsloven, jf ordlyden i personopplysningsloven § 2 nr 8. Opplysningen ligger under Datatilsynets tilsynsmyndighet. Strafferegistreringsloven har ingen bestemmelser om sletting av opplysninger. Utfyllende regler må derfor finnes i personopplysningsloven, jf personopplysningsloven § 5. Nemnda gjennomgår politiets instrukser og praksis, men personopplysningsloven har forrang. Instrukser og praksis kan brukes for å tolke hvor lenge lagring er «nødvendig for å gjennomføre formålet med behandlingen», jf personopplysningsloven § 28. Nemnda finner etter en totalvurdering at i denne konkrete saken er den 20 år gamle opplysningen ikke lenger nødvendig for å gjennomføre formålet

med behandlingen og skal derfor slettes. Nemnda er bekymret over den vide tilgangen til SSP og foreslår at politiet tar i bruk virkemidler for å begrense tilgangen til opplysningene.

PVN-2008-03 OBOS-megleren

Klage på Datatilsynets vedtak om at OBOS-megleren må sørge for tilfredsstillende tilgangsbegrensning i henhold til ansattes tjenstlige behov ved bruken av eMegler

Klage på Datatilsynets vedtak om at OBOS-megleren må sørge for tilfredsstillende tilgangsbegrensning i henhold til ansattes tjenstlige behov ved bruken av eMegler, slik at meglerne kun har tilgang til opplysninger knyttet til sitt eget kontor. Nemnda var ikke enig i Datatilsynets rettsanvendelse og kom til at personopplysningsloven § 11 bokstavene b og d, samt personopplysningsforskriftens § 2-11 ikke krever at tilgangen til eMegler begrenses til det enkelte kontor i denne saken. Klagen ble tatt til følge.

PVN-2008-04 Lindorff

Klage på Datatilsynets vedtak om at Lindorff ikke kan benytte opplysninger om tidligere adresser i kredittvurdering av en privatperson

Klage på Datatilsynets pålegg om at Lindorff ikke kan benytte historiske adresser som variabel i kredittvurdering av en privatperson. Personvernnemnda kom til at når adresse er klassifisert under «kontaktopplysninger», må dette bety at det bare er nåværende adresse som er en korrekt og relevant opplysning. Etter nemndas syn er det en rimelig tolkning av konsesjonen at adresse bare skal brukes til kontakt, ikke som variabel i kredittvurdering. Mindretallet finner også at bare aktuelle adresser kan registreres, men mener at den aktuelle adressen kan brukes som variabel i kredittvurdering.

PVN-2008-05 Creditinform

Klage på Datatilsynets vedtak om at Creditinform må stoppe salg av verdiøkende produkter inntil konsesjon for slik bruk av kredittopplysningsdatabasen foreligger

Klage på Datatilsynets vedtak om at Creditinform må stoppe salg av «bransjeanalyser» inntil konsesjon for slik bruk av kredittopplysningsdatabasen foreligger. Klagen ble tatt til følge. Personvernnemnda mener at bransjeanalyser er omfattet av gjeldende konsesjon. Etter nemndas mening må Datatilsynet av eget tiltak trekke konsesjonen tilbake og regulere salg av tjenesten «bransjeanalyse» i en ny og endret konsesjon dersom tilsynet mener at dette er nødvendig. Det vil ha den konsekvens at alle kredittopplysningsforetak vil bli behandlet likt, i og med at dette er en standardkonsesjon.

PVN-2008-06 Pasient hos fysioterapeut

Klage på Datatilsynets avvisningsvedtak. Klager anmodet Datatilsynet om å gjennomføre et tilsyn hos en fysioterapeut. Dette ble avvist. Klager påklaget avvisningsvedtaket

Klager mener at Datatilsynet skulle ha foretatt tilsyn hos en fysioterapeut som klager har vært pasient hos. Klager hadde klaget fysioterapeuten inn for Helsetilsynet for feilbehandling. Helsetilsynet fikk ikke pasientjournal som det ba om fordi fysioterapeuten hadde fått virus på datamaskinen og ødelagt harddisk. Fysioterapeuten sendte harddisken til IBAS, men IBAS klarte ikke å gjenopprette eller rekonstruere innholdet. Helsetilsynet ga fysioterapeuten en advarsel for brudd på journalforskriften. Etter Personvernnemndas syn, har Datatilsynet gjort det som kan gjøres i denne saken. Klager har fått innsyn i IBAS-rapporten. Når IBAS ikke klarer å gjenopprette eller rekonstruere innholdet på harddisken, er det ikke sannsynlig at andre vil klare det.

8 Regnskap og budsjett for 2008

Personvernnemnda hadde i 2008 en budsjettramme på kr 1 600 000, og fremkommer under kap 1500 Fornyings- og administrasjonsdepartementet i statsbudsjett for 2008.

Totalt forbruk: kr 1 242 341. Personvernnemnda disponerte sin bevilgning til innkjøp av litteratur, tjenester, økonomisk støtte til konferanse, deltakelse på seminar og den internasjonale konferansen, arbeidsgodtgjørelse og reisegodtgjørelse til nemndas medlemmer, lønn til sekretariat og leie av lokaler.

Oslo, 9. januar 2009
For Personvernnemnda
Jon Bing (leder)

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:
Fagbokforlaget
Postboks 6050, Postterminalen
5892 Bergen
E-post: offpub@fagbokforlaget.no
Telefon: 55 38 66 00
Faks: 55 38 66 01
www.fagbokforlaget.no/offpub

Omslagsillustrasjon:
Departementenes servicesenter

Publikasjonen er også tilgjengeleg på
www.regjeringa.no

Trykk: 07 Gruppen AS – 10/2009