Datatilsynet

Datatilsynets årsmelding for 2007

Årsmelding R08/01

11.02.2008

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

Oversendt Fornyings- og administrasjonsdepartementet.

11. februar 2008.

Datatilsynet

Gateadresse: Tollbugata 3, Oslo

Postadresse: postboks 8177, dep

0034 Oslo

E-post: postkasse@datatilsynet.no

Telefon: 22 39 69 00

Faks: 22 42 23 50

Innholdsfortegnelse

DEL I

1 Om Datatilsynet

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

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

Datatilsynet er et uavhengig forvaltningsorgan, administrativt underordnet Fornyings- og administrasjonsdepartementet. 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.

Datatilsynets oppgaver

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

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

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

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

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

2 Organisasjon og administrasjon

Datatilsynets budsjett og rammevilkår

Datatilsynets budsjett var i overkant av 25 millioner kroner, av disse var to millioner øremerket til kommunikasjonsprosjekt. Ca 65 % av det samlede budsjettet går til lønnskostnader, fordelt på 33 medarbeidere. Datatilsynet har pekt på at det er lite rom for å sette i gang tiltak som ikke direkte knytter seg til juridisk saksbehandling eller tilsynsvirksomhet. Overføringen for kommunikasjonsprosjekt er derfor videreført i 2007.

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

Organisasjon

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

- Direktøren
- Juridisk avdeling: 13 medarbeidere
- Tilsyn- og sikkerhetsavdelingen 5 medarbeidere
- Administrasjonsavdelingen 7 medarbeidere
- Informasjonsavdelingen 8 medarbeidere. 4 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. Fire kvinner har i 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 40,9 år for menn og 38,7 år for kvinner.

Tre medarbeidere sluttet i virksomhetsåret.

Datatilsynet ønsker å stimulere til et kulturelt og kompetansemessig mangfold i staben. Videre tilrettelegges det for en personalpolitikk som skal virke motiverende, og hindre utstøting av personer med nedsatt funksjonsevne. Datatilsynet er knyttet til avtalen om inkluderende arbeidsliv. Fokus har også i 2007 vært tiltak som forebygger belastningslidelser. Dette har vært tiltak knyttet til trening, ergonomisk veiledning og instruksjon om hensiktsmessig arbeidsteknikk.

3 Saksbehandling

Det ble journalført 6520 dokumenter i meldingsåret. Av disse var 2952 innkomne og 3404 utgående brev fra Datatilsynet. Resten var journalførte interne notater. Dette er omtrent på samme nivå som for 2006.

Nye saker (som ikke har startet i et tidligere meldingsår) utgjorde 1928, hvorav 1428 ble fordelt til juridisk avdeling, mens 215 og 231 saker ble fordelt henholdsvis til Datatilsynets juridiske svartjeneste og tilsyns- og sikkerhetsavdelingen. Resten av sakene ble fordelt til administrasjonen, informasjonsavdelingen og direktøren.

Av de nye sakene utgjorde 1/3 klager fra publikum. Flest klager kom inn på områdene kredittopplysning, direkte reklame, tele/Internett, arbeidsliv og helse. I meldingsåret mottok tilsynet 506 søknader om konsesjoner. Av disse utgjorde forskning over halvparten av søknadene. Av andre som er verd å nevne er søknader om konsesjon innen forsikring, bank og barnevern. Med unntak av forskningen er dette konsesjoner som i stor grad er standardisert.

I årsmeldingen for 2006 ble det redegjort for konsekvensene av tilknytning til ny forskningslov. Nå ble ikke ny forskningslov vedtatt i 2007, og vil tidligst bli det i 2008, men synspunktene vil ha samme relevans.

En sak som i stor grad preget Datatilsynets saksbehandling var de mange klager fra publikum i forbindelse med ”innhøstingen” av personopplysninger i tilknytning til Tele2-saken. Dette var klager som ble formidlet til oss både brevlig, via e-post og telefon. Datatilsynet anmeldte ett teleselskap i saken.

Konsesjonsplikten

Plikten til å søke konsesjon gjelder i all hovedsak for behandling av sensitive personopplysninger, blant annet opplysninger om helse, rase, religiøs oppfatning, politisk tilknytning, fagforeningstilhørighet, straffbare handlinger og seksuell adferd.

Datatilsynet kan også bestemme at andre behandlinger av personopplysninger skal være konsesjonspliktige, så fremt behandlingen åpenbart vil krenke tungtveiende personverninteresser.

I 2007 ble det gitt 237 konsesjoner.

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 2007 kom det inn 2952 meldinger om behandling av personopplysninger mot 3019 i 2006. Totalt er det nå 8946 meldinger i meldingsdatabasen, mot 8954 året før. 2989 meldinger ble slettet fra databasen i 2007 mot 5518 året før.

Klagesaker til Personvernnemnda

I meldingsåret oversendte Datatilsynet 7 saker til Personvernnemnda for videre klagebehandling: Dette gjaldt:

- Klage på Datatilsynets avgjørelse om tilgang til Det norske tvillingpanelet og om bruk av sanksjoner mot Universitetet i Oslo for ulovlig bruk av personregister

- Klage på vedtak om krav om samtykke for registrering i historisk database – Biblioteksystemer
- Klage på vedtak om at utlegging av eiendomsinformasjon i Asker og Bærums budstikke er å regne som journalistisk virksomhet.
- Elektronisk billettering i Rogaland
- Publisering om personopplysninger om fosterforeldre på internettsiden www.likestilling.no
- Klage på avvisningsvedtak – innsyn i personopplysninger hos OBOS
- Klage på vedtak om bruk av fødselsnummer på www.ung1881.no

Personvernombud

Datatilsynet har også i 2007 hatt fokus på personvernombudsordningen. Antallet nye ombud økte like mye som året før, og tilsynet er stolte over å kunne telle 100 personvernombud.

Den raske veksten stiller også store krav. Tilsynet må sørge for at ombudene føler seg ivaretatt, og at kvaliteten på ordningen er god. For å hjelpe ombudene med faglig påfyll og inspirasjon, har tilsynet startet en ordning med å sende ut månedlige nyhetsbrev til ombudene på e-post. Her kan det for eksempel informeres om vedtak fra Personvernnemnda, arbeid fra artikkel 29-gruppen og interessante artikler kan vedlegges.

Utsendelsen av nyhetsbrevene viser seg også å være et effektivt virkemiddel for tilsynet for å fange opp ombud som ikke lenger er operative. Det er dessverre slik at mange virksomheter glemmer å gi beskjed til tilsynet ved bytte av ombud, for eksempel i forbindelse med at et internt ombud slutter i virksomheten. Datatilsynet har utarbeidet en liste over virksomheter som har personvernombud som er tilgjengelig på tilsynets hjemmeside. Denne skal til enhver tid være oppdatert.

Datatilsynet har gjennomført fire kurs for eksisterende personvernombud i 2007. To av kursene knyttet seg til opplæring av nye ombud. Tilsynet synes det er viktig at nye ombud relativt raskt får et tilbud om grunnleggende personvernrett. Tilbakemeldingene fra ombudene er gode.

29. og 30. mai 2007 ble det arrangert seminar for alle ombud. For første gang ble ombudene delt inn i bransjer i deler av sesjonen, blant annet bank, inkasso, kommuner, privat virksomhet og helsesektoren. En slik inndelingen fordret en stor ressursbruk av tilsynets ansatte. Ombudene var svært fornøyde med denne måten å arrangere seminar på.

To av tilsynets medarbeidere som jobber med personvernombudsordningen var på studietur til Paris. Der deltok de på et seminar som det franske datatilsynet, CNIL, arrangerte, og utvekslet erfaringer med franskmennene.

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. Tilsynet arbeider blant annet for å påvirke at nasjonal og internasjonal lovgivning tar hensyn til respekten for privatsfærens betydning for bevaring av menneskerettigheter, demokratiet og rettsstatens institusjoner.

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

Arbeidsgruppe for revisjon av personopplysningslov og personopplysningsforskrift

Personopplysningsloven skal etterkontrolleres. I denne anledning er det nedsatt en arbeidsgruppe som arbeider med problemstillinger knyttet til lovrevisjonen. Gruppen består av representanter fra Justis- og politidepartementet, Fornyings- og Administrasjonsdepartementet og Datatilsynet. Gruppen hadde en rekke møter våren 2007 der Datatilsynet på forespørsel fra Justis- og Politidepartementet redegjorde for behov for endringer. Høsten 2007 ble det ikke gjennomført nye møter.

Arbeidsgruppe for opprettelse av Offentlig Elektronisk Postjournal (OEP)

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

Samarbeidsråd for helsesektoren

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

Bransjenorm for helsesektoren

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

KIS - Koordineringsutvalget for informasjonssikkerhet

Utvalget består av representanter for sju departementer, Statsministerens kontor og ni direktorater. Opprettelsen av koordineringsutvalget er et ledd i gjennomføringen av Nasjonal strategi for informasjonssikkerhet. Arbeidet omfatter alminnelig IT-sikkerhet og spørsmål knyttet til rikets sikkerhet, vitale nasjonale sikkerhetsinteresser og kritiske samfunnsfunksjoner. Utvalget skal samordne videreutviklingen av IT-sikkerhetsregelverket, få frem felles standarder, normer, metoder og verktøy for IT-sikkerhet og sørge for samordning av tilsynspraksis. Utvalget skal også drøfte aktuelle

risiko- og sårbarhetsspørsmål og bidra til koordinering av informasjonstiltak og beredskapsplanlegging Mye av arbeidet i KIS delegeres til arbeidsgrupper. Datatilsynet har prioritert å være aktiv i disse arbeidsgruppene.

SARI – Samordning av regelverk innen informasjonssikkerhet

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

KOBI – begrepsapparat innen regulering av informasjonssikkerhet

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

Koordineringsutvalget for E-forvaltning

Utvalget skal arbeide med samordning mellom de forskjellige offentlige organer for å realisere planen E-2009. Møtene ledes av Fornyings- og administrasjonsministeren. Arbeidet fokuserer på målene i E-2009, og hvordan de enkelte aktører kan bidra for å realisere disse.

Arbeidsgruppe for implementering av datalagringsdirektivet

Dette er en interdepartemental gruppe for implementering av datalagringsdirektivet.

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

Ny folkeregisterlov

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

Nasjonalt identitetskort, elektronisk signatur og elektronisk identitet

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

NAFAL

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

5 Internasjonalt samarbeid

I likhet med deltakelse i norske offentlige råd og utvalg, er også deltakelse på internasjonale møter og arbeidsgrupper en viktig arena for å påvirke lovgivningen på området. 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. Sammen med kollegaer fra de ti søkerlandene til EU-medlemskap, har Datatilsynet deltatt som observatør i arbeidsgruppen opprettet etter direktivets artikkel 29. Gruppen har som oppgave å drive 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 fire to-dagersmøter i Brüssel, i tillegg til det større "vårmøtet", som denne gang ble arrangert på Kypros.

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

- *Medical Data.* Arbeidsgruppen har hovedfokus på helsejournaler.
- *Identity management.* Arbeidsgruppen tar for seg autentisering og identifisering i den elektroniske verden. Gruppen har ikke hatt møter i meldingsåret.
- *Internet task force.* Arbeidsgruppen arbeider med internettrelaterte spørsmål, med vekt på det tekniske. I meldingsåret har gruppen blant annet jobbet med definisjonen av begrepet "personopplysning" og bruk av søkemotorer på Internett

Det internasjonale datatilsynsmøtet

Hvert år holdes det en internasjonal konferanse for datatilsynssjefer med deltakere fra hele verden. Konferansen inneholder en åpen del som også andre enn datatilsynssjefene kan delta på. I 2007 ble konferansen holdt i Montreal. Datatilsynet deltok med to representanter.

Berlin-gruppen

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

- Søkemotorenes praksis med hensyn til lagring av søk
- Planlagt bruk av det europeiske satellittsystemet Galileo innen samferdselssektoren
- Bruk av RFID i legitimasjonsdokumenter og betalingskort

- Digitalisert overvåking: Internett samt kameraovervåking

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

Police Working Party

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

Joint Supervisory Authority

JSA er det felles tilsynsorganet for Schengen Informasjonssystem (SIS). Informasjonssystemet inneholder opplysninger om personer som er ettersøkt, savnet, nektet innreise til Schengenområdet, eller er straffedømt i et av medlemslandene. Normalt avholdes fem møter årlig i Brüssel, og Datatilsynet er representert med ett medlem i gruppen. I tillegg har en informasjonsmedarbeider bistått i arbeidet med å utvikle informasjonsmateriell knyttet til innføringen av SIS II.

Internasjonalt saksbehandlermøte

Dette er et internasjonalt samarbeidsforum for saksbehandlere. Det ble avholdt to møter, henholdsvis i Helsinki og Lisboa. Diskusjonene omhandlet blant annet behandling av personopplysninger på Internett og bruk av biometri. Begge disse temaene ble vurdert som såpass viktige at de også videreføres til møtene i 2008. I tillegg ble det diskutert bruk av kredittopplysninger i forskjellige sammenhenger, overvåking i arbeidslivet og i samferdselssektoren. 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 år ble møtet holdt på Island.

Nordisk saksbehandlermøte

Dette er et årlig nordisk forum for saksbehandlere. Arrangementet går på rundgang mellom deltagerlandene og i 2007 var turen kommet til Norge. Møtet ble avholdt i Bergen og Datatilsynet var representert med tre saksbehandlere. Møtet hadde særlig fokus på kontroll i arbeidslivet og på samferdselssektoren. I tillegg ble behandling av personopplysninger på Internett diskutert. Nytt av året var at tilsynsmyndighetene på Færøyene deltok med to representanter. Datatilsynet var representert med tre saksbehandlere.

Nordisk teknologimøte

Det ble ikke avholdt møter i meldingsåret.

6 Informasjonsvirksomheten

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

Dette er imidlertid tradisjonelle virkemidler med sine klare begrensninger. Datatilsynet fikk derfor i 2006 bevilget to millioner kroner til å utvikle en ekstra satsing på kommunikasjonstiltak som kan gi både befolkningen som rettighetshavere og virksomheter som plikthavere en økt oppmerksomhet, refleksjon og kunnskap om viktige personvernspørsmål. De øremerkede ekstramidlene for kommunikasjonstiltak ble videreført og ytterligere styrket i 2007, noe som har gitt synlige og dokumentert gode resultater.

Undervisningsopplegget ”Du bestemmer”:

”Du bestemmer” er utviklet av Teknologirådet, Utdanningsdirektoratet og Datatilsynet i et nært og godt samarbeid. Alle disse tre aktørene har bidratt med ressurser til å realisere en utradisjonell og virkningsfull kampanje overfor ungdom som målgruppe. Opplegget er knyttet opp til de nye læreplanene i skoleverket, som inneholder kompetansekrav når det gjelder IKT og personvern.

Undervisningsopplegget ble lansert mandag 29. januar 2007 på et pressearrangement hvor Fornyings- og administrasjonsminister Heidi Grande Røys deltok. Lanseringen ble gjenstand for en betydelig og positiv medieomtale i landsdekkende og lokale medier, samt i fagpressen.

Undervisningsopplegget består av et hefte med faktaopplysninger, historier fra virkeligheten og diskusjonsoppgaver. Det er også laget veggplakater til klasserommet, en multimediepresentasjon med tre humoristiske, men tankevekkende filmsnutter, og en lærerveiledning. Alt dette materiellet, og utfyllende informasjon, kan lastes ned fra nettstedet www.dubestemmer.no.

Det ble ved lanseringen sendt ut prøvepakker på undervisningsopplegget til alle landets ungdoms- og videregående skoler. I forbindelse med nytt skoleår høsten 2007 ble det sendt ut en ny påminnelse om undervisningsopplegget, sammen med to nye filmer. Dette resulterte i en fornyet interesse og en ny strøm av bestillinger. Et nytt, tredje opplag av brosjyren og tilhørende materiell er derfor blitt trykket.

Per 31.12.2007 er det kommet inn mer enn 1 300 bestillinger på samlet over fem tusen klassesett. Dette betyr ca 160 000 utsendte brosjyrer.

Etter oppdrag fra Datatilsynet har TNS Gallup evaluert undervisningsopplegget blant de lærerne som har bestilt materiellet. Resultatene fra evalueringen er meget oppløftende. To av tre lærere vurderer elevenes samlede interesse for tematikken som stor eller svært stor. Like mange sier at materiellet i stor eller svært stor grad førte til diskusjon og refleksjon i klassen. Nesten alle lærerne opplevde at opplegget økte elevenes kunnskap og bevissthet om personvernspørsmål. 78 prosent av lærerne gir opplegget en bra eller svært bra

vurdering som pedagogisk støtteverktøy. Ingen gir undervisningsopplegget en negativ vurdering, og hele 96 prosent av lærerne ønsker å benytte opplegget igjen ved en senere anledning.

Høsten 2007 ble kampanjen presentert for øvrige datatilsynsmyndigheter i Europa på et møte i Berlin. Dette har resultert i flere henvendelser fra land som ønsker å benytte hele eller deler av opplegget. Brosjyren ble som følge av den store interessen også trykket i en engelskspråklig versjon, og de tre filmene fikk engelsk teksting.

I desember mottok Dubestemmer-prosjektet heder og ære i Madrid. Under *European Seminar on Best Practices in Data Protection and Award Giving Ceremony* ble prosjektet tildelt en *First Special Mention,* det vil si at det fikk hederlig omtale.

Prosjektets fase to – ungdom som filmskapere

I løpet av våren 2007 ble elever på Lillehammer videregående skole utfordret til å lage to filmer med personvern og digital mobbing som tema. Elevene skrev manus nært knyttet til situasjoner hentet fra deres egen hverdag. Kortfilmene ble deretter produsert i samarbeid med studenter ved Høgskolen i Lillehammer, og sendes per i dag ut sammen med det øvrige materiellet i klassesettene.

Tilbakemeldingene i evalueringen som ble gjennomført blant lærerne viste at kortfilmene i undervisningsopplegget slo godt an. Lærerne ønsket flere filmer som utgangspunkt for diskusjoner i klassen.

I oktober ble det derfor sendt ut en invitasjon til alle videregående skoler med medielinje om å delta i en manuskonkurranse med personvern og digitale medier som tema. Ungdom kjenner selv best sin egen virkelighet. Film er dessuten en formidlingsform som når frem til denne gruppen. Håpet er at tematikken som berøres i de nye filmene ytterligere vil bidra til å øke ungdoms bevissthet og kunnskap om eget og andres personvern.

Blant alle manusene som kom inn, valgte en jury ut vinnermanusene. I desember ble de seks vinnergruppene samlet i Oslo for en workshop der de videreutviklet manusene etter råd fra filmfaglige mentorer. Filmene gikk deretter til produksjon på skolene, og hele tiden har elevene tilgang til filmfaglig hjelp. De seks nye filmene har premiere mars 2008 og vil deretter bli sendt ut til alle landets skoler, i tillegg til å bli lagt ut på Internett.

Datatilsynet har også gått inn som hovedsponsor for Amandusfestivalen 2008, en filmfestival for unge filmskapere under 20 år. Arrangørene inviterte derfor til manuskonkurranse med personvern og digitale medier som tema. Vinnermanuset vil filmatiseres av studenter på Den Norske Filmskolen og får premiere på Amandusfestivalen i mars 2008. De seks filmene som produseres i regi av Dubestemmer-prosjektet vil også bli vist på festivalen.

Med dette håper Datatilsynet å møte ungdommen der de er, på deres arenaer, og kunne skape en økt interesse for og en bevissthet rundt temaet personvern.

Opplæring og veiledning overfor virksomhetene

Det er gjennom flere års tilsynsvirksomhet blitt dokumentert et behov for å motivere og legge til rette for økt etterlevelse av personvernlovgivningen i virksomheter som behandler personopplysninger. Dette gjelder offentlige så vel som private.

Takket være de ekstra ressursene til betalt kommunikasjon, ble Datatilsynet satt i stand til å gjennomføre informasjonstiltak også overfor norske virksomheter. Målet har vært å øke virksomhetenes kjenneskap til regelverket og pliktene om internkontroll og informasjonssikkerhet.

Det er blitt utarbeidet et nytt og omfattende veiledningsmateriell, blant annet:

- Motivasjonsheftet *Pokerfjes*
- En fullstendig veileder for internkontroll
- Ulike maler for dokumenter til bruk i internkontrollen
- Tilpasset materiale for virksomheter som kun har personopplysninger om egne ansatte og kunder
- Et støtteverktøy som hjelper virksomheten med å kontrollere egen etterlevelse av de lovpålagte pliktene

I tillegg ble det kjørt en kampanje overfor utvalgte bransjer. Ansvarspersoner i konkrete bedrifter ble kontaktet med tilbud om oppfølging og veiledning, blant annet gjennom seminarer i Trondheim, Bergen og Oslo. Seminarene ble fulltegnet.

Selv om det er blitt utarbeidet et faglig godt og gjennomarbeidet veiledningsmateriale, er Datatilsynets inntrykk at materialet i alt for liten grad er blitt tatt i bruk av norske virksomheter. Dette skyldes trolig at virksomhetenes ledelse ikke har tilstrekkelig forståelse for hvorfor dette er viktig. Både offentlige og private virksomheter vegrer seg mot å prioritere ressurser til arbeidet. Det blir derfor i praksis nedprioritert inntil det kommer tilsynsbesøk fra Datatilsynet, eller det inntreffer en hendelse som oppfattes som kritisk fra virksomhetsledelsens side. Masseinnhøstingen av fødselsnumre og andre personopplysninger fra ulike teleoperatører sommeren 2007 er et eksempel på dette. Likeledes kommuners ukritiske publisering av personopplysninger på Internett.

Ved bruk av kommunikasjon og dialog er det mulig å skape betydelige resultater, slik kampanjen overfor ungdom har vist. Datatilsynet mener derfor at det bør settes av ressurser til å utvikle presentasjonsmateriell som på en overbevisende måte motiverer til igangsetting av arbeidet med internkontroll og informasjonssikkerhet. Videre bør det satses ytterligere på ordningen med personvernombud.

Personvern uttrykt gjennom kunst

Fornyings- og administrasjonsdepartementet bevilget sommeren 2007 ekstra midler til et prosjekt hvor personvern skal uttrykkes gjennom kunst. Tanken er at man ved å involvere kunstneriske uttrykk utvider debatten om personvern, privatliv, integritet og overvåkingssamfunnet. Tradisjonelt har kunstnere hatt en viktig rolle i samfunnsdebatten. Kunstprosjektet kan derfor løfte problemstillingene og tilføre noe nytt, tankevekkende og viktig. For å ivareta den kunstfaglige kompetansen er det i inngått et samarbeid med KORO, Kunst i offentlige rom. Det arrangeres en åpen idékonkurranse med arbeidstittelen ”Respekten for privatlivets fred” som vil være åpen for forskjellige uttrykk innen visuell kunst.

Konkurranseutlysningen blir foretatt i februar 2008. Utstillingen av de ferdige verkene vil finne sted høsten 2008 på Oslo sentralstasjon.

Personvernrapporten fikk stor oppmerksomhet

For fjerde gang ble det laget en publikasjon som populariserer noe av innholdet fra årsmeldingen for forutgående år, men som også skuer fremover. *Personvernrapporten 2007* ble trykket i ni tusen eksemplarer og distribuert til ca 5 700 mottakere. Datatilsynet lanserte Personvernrapporten ved å arrangere en pressefrokost i april. Det møtte opp femten journalister fra en rekke medier, både aviser, tv og radio. Det ble på pressefrokosten gitt hele 21 ulike intervjuer, som alle resulterte i nyhetsoppslag. Personvernrapporten har utelukkende fått positiv omtale.

På grunn av et langt større antall etterbestillinger enn tidligere år ble det i august trykket opp et ekstra opplag på 2 000 eksemplarer. Per 31.12.2007 var det kommet inn 626 etterbestillinger av til sammen 2 165 eksemplarer.

Datatilsynets hjemmeside

Hjemmesiden www.datatilsynet.no er på mange måter selve navet i Datatilsynets informasjonsvirksomhet. Det legges derfor stor vekt på å bruke nettsiden aktivt.

Det ble produsert 85 egenproduserte nyhetssaker i 2007. I tillegg har Datatilsynet fortsatt den planmessige oppbyggingen og gjennomgangen av informasjonen om sektorer og spesifikke teknologier.

Datatilsynet sender e-postvarsel når forsiden oppdateres til 3 053 abonnenter som selv har meldt seg på varslingslisten.

Personvernrapporten 2007 ble i meldingsåret lastet ned mer enn 10 500 ganger. Telefonsalg og reklame er det undertemaet som leses mest på nettsiden.

Datatilsynets hjemmeside ble i 2007 vurdert til en lavere poengsum enn tidligere (fra fem til tre stjerner) i norge.no sin kåring av offentlige nettsteder. Delvis skyldes dette strengere krav til tilgjengelighet. Datatilsynet ser tilgjengelighet som et essensielt mål, og har allerede bestilt utbedringer av løsningen.

Datatilsynet ble også trukket for at ikke fulltekstdokumenter/postliste ligger tilgjengelig på nett, at tilsynet ikke har deler av sine saksbehandlingssystemer tilgjengelige fra Internett, eller har avanserte toveisløsninger mot borgeren. Slike løsninger utgjør imidlertid en betydelig sikkerhetsmessig risiko. Som tilsynsmyndighet på dette området må Datatilsynet vise spesiell varsomhet. I tilsynspraksisen erfarer Datatilsynet at flere av de løsninger som benyttes i dag ikke tilbyr god nok sikkerhet for at det kun er rette vedkommende som får tilgang til opplysningene. I tillegg har mange aktører problemer med å kvalitetssikre utleggelsen av dokumenter. Det medfører at opplysninger som ikke skulle vært publisert, likevel havner på Internett. Dette kan medføre store konsekvenser for de som blir utsatt for dette.

Tilsynet har spilt inn en del konkrete råd til departementet når det gjelder e-forvaltning. I tillegg har tilsynet søkt om midler til et prosjekt som kan munne ut i en beste-praksismetode for hvordan hensynet til personvern og ønsket om effektivitet og aktiv publisering av saksdokumenter kan forenes.

Mediekontakt

Ved siden av hjemmesiden er en aktiv mediekontakt et svært prioritert virkemiddel for å skape oppmerksomhet og debatt omkring behovet for å respektere også personvernhensyn når nye teknologier og velmente tiltak skal iverksettes. Som ledd i dette har Datatilsynet

sett det som viktig å utvikle en organisasjon og kultur som gjør at mange medarbeidere føler seg rustet til å gi uttalelser innen egne saksområder til media, og delta i debatter på radio og tv. På denne måten har Datatilsynet, sett i forhold til organisasjonens størrelse, stor kapasitet til å kunne tale personvernets sak når anledningen byr seg.

I løpet av meldingsåret har Datatilsynet besvart over 1 350 henvendelser fra mediene, i form av å gi intervjuer, eller delta i debatter. Dette har resultert i over fem tusen registrerte medieoppslag hvor Datatilsynet er omtalt.

Av saker som har fått særlig medieomtale kan nevnes:

- Det sosiale nettverkstedet Facebook
- Fødselsnummer, herunder masseutlevering av personopplysninger
- ID-tyveri
- Personvernrapporten
- Tilganger til helseopplysninger, brudd på taushetsplikt
- Bruk av fingeravtrykk og annen biometri
- Lansering av undervisningsopplegget ”DuBestemmer”
- Nakenscanner på flyplasser
- NAV – og tilgang til journaler

Datatilsynet har i 2007 også hatt inne flere egenproduserte kronikker og debattinnlegg.

Foredragsvirksomhet

Datatilsynet tilbyr ikke egne seminarer eller kurs ut over det som blir arrangert i forbindelse med personvernombudsordningen. Unntak fra dette var kursene som ble kjørt våren 2007 i forbindelse med den ekstra kommunikasjonssatsingen overfor virksomheter om etablering av system for internkontroll. Datatilsynet stiller imidlertid så langt som mulig opp med foredragsholder når det kommer forespørsler om dette til seminarer i regi av andre. Datatilsynet har som følge av dette vært representert med foredragsholdere på 140 ulike seminarer og konferanser. Nedgangen i forhold til året før er en konsekvens av en helt bevisst og strengt nødvendig prioritering.

	2005	2006	2007
Antall foredrag	92	157	140

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 publikumshenvendelsene blir derfor besvart av en juridisk svartjeneste, bestående av fire jurister. Disse trekker på teknologisk kompetanse når de ser behov for det. I tillegg bidrar de også med vanlig juridisk saksbehandling, i den grad dette ikke går ut over tilgjengelighet og service i veiledningsarbeidet.

Den juridiske svartjenesten har i 2007 registrert 7 300 besvarte telefonhenvendelser, mot tilsvarende 8 125 året før. Nedgangen skyldes hovedsakelig færre henvendelser om innsyn i e-post og direkte markedsføring. I tillegg skyldes nedgangen trolig også at publikum i stadig større grad blir fortrolige med å benytte Internett for å innhente kunnskap og veiledning, fremfor å ty til telefonen.

Tilgjengelighet/svartid på telefonservicen vurderes gjennomgående å være meget god. Tilsvarende også kvaliteten i den veiledningen som gis.

Hva handler henvendelsene om?

Tabellen nedenfor viser telefonhenvendelsene besvart av den juridiske svartjenesten. Henvendelsene er fordelt på tema, og hvorvidt innringer opptrer som (eller på vegne av) plikt- eller rettighetshavere.

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

Den prosentvise fordelingen er ikke direkte sammenliknbar med forutgående år. Dette skyldes blant annet at det er gjort enkelte endringer i temakategoriene. Det gjøres også oppmerksom på at Tilsyns- og sikkerhetsavdelingen besvarer en del henvendelser om informasjonssikkerhet, til sammen 1070 henvendelser i meldingsåret. Disse er ikke med i den omtalte oversikten.

Arbeidsliv er fortsatt det temaet det kommer flest henvendelser om, selv om det har vært en nedgang fra året før. I tillegg til spørsmål om rutiner for arbeidsgivers innsyn i e-post, logging av datamaskinbruk mv, inngår henvendelser om kameraovervåking og andre systematiske kontrolltiltak fra arbeidsgivers side.

Det er også verdt å merke seg en fortsatt og markert nedgang i antallet henvendelser om direkte markedsføring, særlig knyttet til reservasjonsregisteret. Datatilsynet mottok 505 telefonhenvendelser fra rettighetshavere i 2007. Dette utgjør en tredel av antallet henvendelser tre år tidligere. Som tidligere nevnt var imidlertid telefonsalg og reklame det temaet som var mest lest på Datatilsynets hjemmeside i 2007. En forklaring på nedgangen i antallet henvendelser om direkte markedsføring kan dermed dels skyldes at publikum finner svar på sine spørsmål på nettet, fremfor å ringe eller skrive e-post til Datatilsynet.

År	**2004**	**2005**	**2006**	**2007**
Antall telefonhenvendelser om DM	1 496	838	617	505

Det har vært en fortsatt økning i antallet henvendelser vedrørende informasjonssikkerhet og fødselsnummer. Dette skyldes et økt fokus i mediene på saker om manglende informasjonssikkerhet, masseinnhøsting av fødselsnummer fra teleselskaper mv.

Henvendelser per e-post

Det har kommet inn 2 673 henvendelser per e-post til den juridiske svartjenesten, mot 3 058 året før.

Den juridiske svartjenesten har som mål at gjennomsnittlig svartid på e-post ikke skal overstige to virkedager etter at henvendelsen kom inn til avdelingen. Ingen e-post skal liggende ubesvart lengre enn fem virkedager. I en periode var svartidene lengre enn dette, men dette ble i løpet av høsten brakt under kontroll. Ved årsskiftet var det ingen ubesvarte e-posthenvendelser.

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.

Tilsyns- og sikkerhetsavdelingen besvarte 429 e-posthenvendelser i 2007.

7 Tilsyns- og sikkerhetsarbeid

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

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

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

- Kontakt med aktuell bransjeforening eller andre bransjeorganer for å drøfte lovforståelse og tolkning, initiere bransjenorm eller publisere fagartikler i medlemsblader.
- Kontakt med eierinteressene.
- Beskrive problemer i media, lage veiledninger som legges ut på tilsynets hjemmeside, eller bidra med foredragsvirksomhet.
- Starte prosjekter hvor de nye problemstillingene kan gjennomgås.

7.1 Funn i flere sektorer

Informasjonsteknologien er fremdeles i en tidlig fase når det gjelder spørsmålet om intern sikkerhet og samhandling. Virksomhetene føler et behov for å bruke sine IT-systemer til å skape bedre informasjonsflyt – også når det gjelder personopplysninger. Nødvendige mekanismer for intern sikkerhet og trygg samhandling har imidlertid ikke vært på plass.

Problemstillingen har i hovedsak fem dimensjoner:

- Antall medarbeidere som har tilgang til personopplysninger
- Tidsrommet disse har tilgang
- Mengden informasjon den enkelte har tilgang til
- Kontrollmekanismene omkring ansattes bruk av personopplysninger
- Sikkerhet knyttet til kundenes tilgang til egne opplysninger

Datatilsynets kontrollvirksomhet indikerer at mange virksomheter kommer dårlig ut i forhold til flere av disse dimensjonene. Dette representerer en markant trussel mot den enkeltes personvern. Det at virksomhetene er for lite restriktive med hvilke ansatte som får tilgang, kombinert med manglende kontrollmekanismer med hvem som gjør oppslag, utgjør trolig den største enkeltrisikoen.

Den manglende sikkerheten rundt kundenes tilgang til egne opplysninger følger som en god nummer to. I de fleste tilfeller kreves det kun en svak autentisering av kunden før det gis tilgang til personopplysningene.

Brudd på bestemmelsene om informasjonssikkerhet og internkontroll er like fremtredende som tidligere år. Gjennomgående sliter virksomheter med å dokumentere sikkerheten slik regelverket foreskriver.

Trolig forekommer krenkelser av noens personvern daglig, uten at det blir kjent for den fornærmede. Det kan være uautorisert innsyn i ulike typer sensitive personopplysninger, eller gjenbruk av personopplysninger uten at nytt behandlingsgrunnlag foreligger. Det er ofte svært vanskelig å avdekke slike krenkelser, delvis fordi dette skjer i lukkede miljøer, og delvis fordi systemene ikke er egnet til en effektiv kontroll av misbruk.

Datatilsynet merker seg at respekten for bestemmelsene om sletting gjennomgående er lav. Dette gir grunnlag for bekymring, spesielt når terskelen for å registrere opplysninger også er lav. Få virksomhetsledere synes å ha vurdert behovet for å slette personopplysninger. Mange hevder at langvarig oppbevaring kan være nyttig for virksomheten. Dermed befinner vi oss i en situasjon der flere og flere virksomheter lagrer flere opplysninger om individet - over stadig lengre tid.

I tillegg skyldes lagringen et langt på vei uavklart forhold til regnskapslovgivningen som pålegger lagring av visse typer opplysninger i en gitt periode.

Det blir generert betydelige mengder overskuddsinformasjon. Regelverket forutsetter at informasjonen som lagres samsvarer med formålet og skal være saklig. Informasjonssystemer som utvikles bygges i mange tilfeller ikke etter dette prinsippet. Tvert imot lagres alle de opplysninger systemet gir rom for, uten at de ansvarlige i det hele tatt synes å reflektere over det.

Nærmere omtale av tilsynene er tatt inn i fagdelen, del II.

7.2 Nøkkeltall fra kontrollvirksomheten

Datatilsynets kontrollvirksomhet omfatter kontrollaktiviteter mot i alt 134 virksomheter.

Følgende bransjer (eller temaområder) var underlagt tilsyn i 2007:

Bransje / Sektor	**Antall**
Arbeidsliv	1
Biometri	1
Eiendomsmeglere	6
E-signatur	2
Finanssektoren	1
Forskning	7
Fjernsynsovervåking	25
Fødselsnummer	15
Helse	7
Internett	14
Justissektoren	1
Kommune	6
NAV	4
Nettcafé	2
Offentlige nettsteder	5
Rekruttering	3
Rusomsorg	10
Samferdsel	2
Sletting	16
Statlig innkreving	3
Telekommunikasjon	2
Trossamfunn	1
Sum	**134**

DEL II

8 Temaer og tendenser i 2007

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 gjennom saker som Datatilsynet er blitt oppmerksom på gjennom medieomtale. Beskrivelsen av tendensene bygger på en grundigere omtale andre steder i årsmeldingen.

8.1 Personvernet er under press

Personvernet er under press på nær sagt alle områder hvor det er gjennomført tilsyn i inneværende år. Når man ønsker å innføre et nytt tiltak, og personvernet oppfattes som en hindring, ser det ut til at mange glemmer at personvernet samtidig må ses på som en viktig garanti for en redelig behandling av personopplysninger. I praksis ser Datatilsynet at personvernet ofte må vike, uten at man vurderer konsekvensene av at denne garantien svekkes eller fjernes.

Presset kommer fra flere retninger. Den ene er en ”klassisk Orwellsk” overvåking, der en Storebror, eller kanskje ”småbrødre”, overvåker andre systematisk som et ledd i sin kontroll og maktutøvelse. Datalagringsdirektivet kan stå som et eksempel på et slikt tiltak.

Den andre pressfaktoren kommer fra omsorgsovervåkingen. I omsorgsovervåkingen blir Storebror erstattet av en ”Store Mor”. Mange gode hjelpere vil beskytte vår helse, økonomi, utdanningsnivå og velferd. Forutsetningen for hjelp er at hjelperne får tilgang til for eksempel helseopplysninger, opplysninger om psykososial velferd, mappen fra barnehage og skolegang, spillevaner og medisinbruk. Dersom de voksnes behov ikke kan begrunne et tiltak, kan kanskje beskyttelsen av det forsvarsløse barnet være grunn god nok?

Effektivisering er en tredje kilde til betydelig press mot personvernet. Det virker som det å vise hensyn til den menneskelige faktoren i seg selv blir oppfattet som en hindring for effektive løsninger. Man ønsker i stor grad å forsyne seg med de opplysningene man mener man trenger. Man vil ikke ta seg bryet med å informere eller spørre den opplysningene gjelder, eller den opplysningene stammer fra. Man vil ha personopplysningene enkelt tilgjengelige for alle i sitt datasystem, og ikke ta hensyn til at mennesker er grunnleggende nysgjerrige. Man vil ikke ta seg bryet med å etablere tilgangskontroll og et forsvarlig sikkerhetsnivå. Resultatet er at borgeren mister kontrollen med hvem som har tilgang til informasjonen om ham.

Datatilsynet er sterkere bekymret for utviklingen ved utgangen av meldingsåret enn tidligere år. Ansvarsfølelsen har vist seg å være liten hos mange aktører. I tilsynsrapport etter tilsynsrapport påpekes manglende oversikt over og kontroll med personopplysninger. Problemstillingen blir ytterligere aktualisert ved utsetting av driftsoppgaver og IT-systemer til eksterne leverandører. Datatilsynet har gang på gang sett at behandlingen av personopplysninger settes bort til databehandlere uten tilfredstillende avtale, og uten at man har forvisset seg om at opplysningene er forsvarlig sikret.

Offentlige og private virksomheter kan i stor grad skyve konsekvensene ved å tilby de registrerte et dårlig personvern over på kunden, pasienten eller brukeren. Når et menneske har blitt utsatt for krenkelser bærer han selv tapet – i tid, penger og psykiske påkjenninger. Disse tapene blir ikke reflektert i regnskapene til virksomhetene. Nedprioritering av personvern kan dermed være et etisk betenkelig valg som likevel forsvares ut fra ren bedriftsøkonomisk veiing av kostnader og inntekter. Det har vært få saker hvor fornærmede har reist erstatningssøksmål mot en behandlingsansvarlig.

Datatilsynets kontroller er ikke nok til å få virksomhetene til å etterleve regelverket. Det kreves forståelse av behovet for et godt personvern hos virksomhetene selv, og et våkent publikum som reagerer på overtramp. Tall fra personvernundersøkelsen fra 2005 tyder på at folk flest har tillit til virksomhetene. Dersom man skal legge Datatilsynets funn til grunn, er mange virksomheter, både offentlige og private, ikke denne tilliten verdig.

8.2 Anonyme alternativer forsvinner

Datatilsynet har gjennom flere årsmeldinger påpekt tendensen til at de anonyme alternativene er under spesielt press. I meldingsåret ble det bestemt at bomringen i Oslo ikke lenger skal ha en anonym passeringsmulighet. Det reelt anonyme alternativet, myntbetalingen, tas bort, og bommen blir helautomatisk.

I flere fylker ser man en oppbygging av sporbar elektronisk billettering i kollektivtransporten.

Løsninger der personlige, elektroniske brikker erstatter ihendehaverbevis som klippekort, dagsbilletter eller kontanter, medfører en betydelig fare for personvernet. Datatilsynet mener det bør være mulig å lage de elektroniske løsningene på en slik måte at man ikke knytter elektronisk billett eller brikke til én bestemt person. I praksis ser tilsynet likevel at viljen til å lage slike løsninger er bortimot fraværende. Offentlige og private virksomheter ønsker i stor grad å kunne følge den enkelte personen i sine systemer.

I meldingsåret kom det også frem et forslag om pliktig registrering av selve brukeren til telefonen, ikke bare abonnenten. Her ble omsorgen for mobilbrukere under 18 år anført som årsak til å gjennomføre en endring som berører alle. Datatilsynet uttalte seg tvilende til at en pliktig registrering av barn vil føre til færre uønskede henvendelser rettet mot dem. Tvert imot mener tilsynet at flere foreldre ønsker at mobilabonnementet skal stå på dem, nettopp for å beskytte barna. Registreringen av brukeren har da også i flere tilfeller ført til at barn, uten de foresattes viten, er blitt oppført med fullt navn og mobilnummer på nummeropplysningstjenester. Sikkerheten for barnet har dermed ikke blitt bedret.

8.3 Personopplysninger blir ikke slettet

Lagring av elektroniske data er blitt billigere enn å ha rutiner for sletting. Datatilsynet så spesielt på sletting i meldingsåret, og avdekket manglende respekt for slettebestemmelsene på nær sagt alle områder. Så å si alle tilsyn førte til merknader. Virksomhetene velger ofte minste motstands vei, videre lagring og større harddisker.

Overgangen fra kontant betaling til elektroniske betalingsmetoder ser man innenfor de aller fleste samfunnssektorer. Stadig oftere tar man vare på all informasjonen man har, i stedet

for kun å lagre det som er nødvendig etter regnskapslovgivningen. Som hjemmelsgrunnlag vises det til regnskapslovgivningen. Det vil si at detaljopplysninger som før ikke ville blitt lagret, eller som ville blitt lagret i kort tid, nå i stedet lagres i minst ti år. Dette så Datatilsynet ved tilsyn blant annet hos nettbutikker og hos hoteller. I meldingsåret kom det også frem at flere fylkesskattekontorer ba om innsyn i gamle passeringsopplysninger hos bompengeselskapene. Man kan lese mer om disse sakene i fagdelen, kapittel ni.

I tillegg ser Datatilsynet en manglende vilje til å utbedre feil i systemer som eksisterer. Politiet har ikke slettet eller sanert opplysninger om pågripelser og reaksjoner i Det sentrale straffe- og politiopplysningsregisteret (SSP) etter 2001. Årsaken er en teknisk feil, og evnen til å utbedre registeret synes fraværende. Dette fører til at rettighetene til de registrerte blir neglisjert.

8.4 Snoking blir ikke avdekket

Datatilsynet har i meldingsåret fått inn flere henvendelser fra enkeltmennesker som mener at bankansatte, fengselsansatte, helsepersonell og politi går inn i databaser og leser opplysninger om dem, uten å ha tjenstlig behov. Datatilsynet har kunnet undersøke en del av påstandene, og funnet at de stemmer.

Mørketallene på området er trolig store. Svært mange virksomheter har mangelfull kontroll med hvem som slippes til i databasene, og altfor få kontrollerer loggene i etterkant. Derfor vil snokingen i mange tilfeller være vanskelig å avdekke.

Svært mange virksomheter åpner for videre tilgang til databasene enn det som var mulig tidligere. Mer enn 13 000 personer har tilgang til politiets sentrale straffe- og politiopplysningsregister (SSP). Antallet NAV-ansatte som kan gå inn i fagsystemene til tidligere Trygdeetaten, sosialtjenesten og Aetat er trolig doblet etter sammenslåingen. For bankene har vi ikke gode tall, men også her har svært mange tilgang til opplysningene om alle kundene.

I praksis har Datatilsynet sett at sykehus og bankvesen tilbyr bedre beskyttelse til kjendiser. Datatilsynet antar imidlertid at en god del av de uberettigede oppslagene gjelder snokerens egen bekjentskapskrets, ikke kjendiser. Samme type beskyttelse bør derfor kunne tilbys alle som ønsker det.

I meldingsåret sendte Helse- og omsorgsdepartementet ut et lovforslag som tydeliggjør at helsepersonell ikke kan lese andres helseopplysninger uten tjenstlig behov. Datatilsynet er fornøyd med forslaget, men foreslår at man vurderer å ta inn et supplement, at alle pasienter får en rett til kostnadsfritt å se hvem som har slått opp i deres journalopplysninger.

Når virksomhetene selv kontrollerer loggene, kan en del oppslag være vanskelig å identifisere som snoking. Personen det gjelder vil ha bedre forutsetninger. Tilsynet mener at en slik rett til å få vite hvem som har hatt tilgang til opplysningene i databasene, også bør gjelde overfor flere aktører.

8.5 Datainnhøsting er blitt enklere – store lekkasjer i meldingsåret

8.5.1 Datainnhøsting

Datainnhøsting er innsamling av store mengder personopplysninger, enten for egen bruk, eller for på videresalg. Flere faktorer ligger til rette for at innhøsting av informasjon om deg og meg er enklere enn det bør være i Norge. Én ting er å høste inn informasjon den enkelte har publisert om seg selv, frivillig, og med åpne øyne for at slik nedlasting vil skje. Noe helt annet er innhøsting av informasjon den enkelte ikke engang visste var tilgjengelig for alle, eller informasjon man plikter å gi fra seg til helt andre formål.

Kombinasjonen av for svak sikkerhet og liberal praksis med publisering av personrelatert informasjon danner et trusselbilde som gir grunnlag for uro. Datatilsynet opplever at aktørene ofte beveger seg i gråsonen for hva som kan være forsvarlig. Hensynet til brukervennlighet, kostnader og dynamikk gjør at man velger et for lavt sikkerhetsnivå, og dermed skaper unødvendige personverntrusler.

I 2007 ble det vist i praksis at slik innhøsting kan gjennomføres i Norge, at noen er villig til å gjøre det, og at det kan få store konsekvenser. Omlag 180 000 nordmenn ble rammet av denne datainnhøstingen.

Innhøstingen av personopplysninger skjedde ved at noen kjørte et dataprogram mot utvalgte nettsider. Ved hjelp av et annet dataprogram hadde de generert fødselsnumre som kunne være i bruk i Norge. Disse ble senere sjekket mot en offentlig nettside for å luke ut numre som ikke er tildelt en person. Fødselsnumrene ble brukt til å søke frem innehaverens navn og adresse via flere teleselskapers nettsider.

De fleste berørte hadde aldri hatt noe med de aktuelle teleselskapene å gjøre. Datatilsynet opplevde mange telefoner fra sinte nordmenn som ikke kunne forstå at dette var mulig. Saken skapte debatt i media, i styrerommene og hos tilsynsmyndighetene.

De som gjennomførte dette, satt tilbake med en grunndatabase som trolig vil ha en varig verdi. En base som inneholder fødselsnummer, med andre ord en offisiell, varig og entydig identifikator, navn og andre kontaktopplysninger til kredittverdige nordmenn. Med en database av såpass høy kvalitet, kan man med relativt god treffsikkerhet føye til annen informasjon. For eksempel fra norske skattelister, som man finner anrettet for enkel nedlasting på Internett, eller fra andre aktører med som tilbyr dårlig beskyttelse av personopplysninger.

8.5.2 Offentlighetsloven

Den nye offentlighetsloven legger opp til at offentlige i større grad enn før skal kunne gjøre sine dokumenter tilgjengelige på Internett. Gjennom publisering av postlister og dokumenter på nettet, har mange aktører i offentlig sektor gjort spørsmålet om offentlighet til et globalt anliggende. Det norske domenet .no er tilgjengelig for hvem som skulle ønske det, i Kirkenes, Lindesnes eller New Dehli. Leseren trenger heller ikke være et menneske. Det kan være maskiner, roboter, som skanner gjennom sidene, indekserer innholdet og bevarer det for fremtiden. Muligheter til å høste inn og systematisere informasjon om nordmenn kan gjøres fra hvor som helst i verden.

Søkemotorene er for lengst identifisert som mulige trusler mot personvernet. Søkemotorene har blitt svært kraftige, og gjør personopplysninger tilgjengelige i samlet form, til tross for

at de i utgangspunktet er publisert hos ulike aktører. All samhandling med offentlig sektor som innbyggeren har, og som ikke er unntatt offentlighet, vil være tilgjengelig ved søk på navn – med mindre det er satt i verk vern mot dette.

I tillegg til det materiale som legges ut med rette, er det en andel som legges ut ved en feiltakelse, manglende opplæring eller regelrett slurv. De som samler inn informasjon ser naturligvis ikke forskjell på tilsiktet og ikke-tilsiktet publisering. De trenger ikke engang å forstå norsk.

Det eksisterer allerede i dag kommersielle virksomheter som gjennomsøker nasjonale domener etter personopplysninger, samler disse inn og systematiserer informasjonen. Formålet er å samle tilstrekklig informasjon til at det foreligger en betalingsvilje. Virksomheten kan dermed selge informasjon om individet som er samlet inn over tid fra for eksempel offentlige postlister og dokumenter. Dersom disse virksomhetene er lokalisert utenfor EØS-området, vil det være svært vanskelig å håndheve rettigheter nordmenn er gitt i personopplysningsloven.

8.6 Økt fare for identitetstyveri i Norge

Når det legges til rette for enkel datainnhøsting, blir befolkningen sårbar for identitetstyveri. Etter gjennomgangen i punktene over, spør Datatilsynet om man ikke i realiteten er i ferd med å anrette en stående buffé for identitetstyver.

Personopplysninger har fått omsetningsverdi i kriminelle miljøer. Dess større mengder informasjon en ID-tyv klarer å skaffe tilveie, dess større sjanse har han til å lykkes med å opptre som en annen person. Å ha et legitimasjonsdokument vil i de fleste tilfeller virke overbevisende. Dersom identitetstyven i tillegg kan supplere med detaljert informasjon om offeret, er veien kort til ”gyldig identifisering”.

En metode som er velkjent for å skaffe tilgang til personlige dokumenter har vært å omadressere post. Inntil ganske nylig hadde Posten Norge AS et lavterskeltilbud for å endre postadresse. Kun tilgang til fødselsnummer og eksisterende postnummeradresse var nødvendig for en slik omadressering. Etter påtrykk fra blant annet Datatilsynet er dette nå endret. Det er imidlertid fortsatt enkelt å endre adresse. Det holder å ta en telefon til Posten.

For å minske sårbarheten for datainnhøsting og ID-tyveri må man beskytte personopplysninger bedre, også de som ikke er kategorisert som sensitive.

I meldingsåret fikk man en debatt om testing av sikkerhet på nettsider. En forskergruppe ved Universitetet i Bergens testet sikkerheten i bankenes elektroniske ID-løsning, BankID. Forskerne publiserte sine funn, og ble møtt med massiv kritikk fra blant annet bankene og Post- og teletilsynet. Datatilsynet mener det er viktig med aktive forskningsmiljøer som sammen med tilsynsmyndighetene identifiserer svakheter i slik sentral infrastruktur. Datatilsynet opplever for egen del at mange virksomheter ikke tar advarsler som blir meddelt dem til følge, og at det først er etter omtale i media at det kommer til handling. Tilsynet har derfor forståelse for at forskere finner det naturlig å gå offentlig ut med advarsler som ikke er tatt på alvor hos aktørene. Forskerne har en meget viktig rolle i forhold til å bidra til å utvikle infrastrukturen i en positiv retning.

Datatilsynet har merket seg at lovforslaget som følger datakrimutvalgets delrapport II kan utløse vanskelige problemstillinger rundt forskernes rolle i fremtiden. Hva som anses som

kriminell adferd defineres så uklart at samfunnskritisk forskning innen teknisk infrastruktur kan bli skadelidende. Les mer om dette i avsnittet om justissektoren.

8.7 Blir vi tryggere av inngripende tiltak?

Perioden etter årtusenskiftet har vært preget av hendelsene 11. september 2001. Medieoppslag om terror, trusler og vold evner å sette til side selv de mest overbevisende forskningsresultater og statistikker.

I iveren etter å gi innbyggerne følelse av trygghet, har myndighetene i flere vestlige land gått svært langt. Mange er villige til å gå på akkord med grunnleggende prinsipper, selv om de bare oppnår marginal reduksjon i risiko.

For sterk kontroll med innbyggerne er en trussel mot rettssikkerhet, frihet og demokrati. Det sentrale i et demokrati er ikke at staten skal overvåke innbyggeren, men tvert imot at innbyggeren skal kontrollere staten. Det er kun på denne måten vi kan forvisse oss om at statsmakten holder seg innenfor akseptable rammer.

Vi har vært vant til at ordensmakten iverksetter tiltak for å etterforske, tiltale og dømme kriminelle. Ved introduksjonen av datalagringsdirektivet er denne forestillingen snudd 180 grader rundt. Direktivet forutsetter at informasjon om bruk av elektroniske kommunikasjonskanaler for alle landets innbyggere, ikke bare for dem som er mistenkt for noe, omhyggelig skal loggføres. Dette gjøres i tilfelle det skulle bli nødvendig å etterforske noen av oss i etterkant. Direktivet krever en lagringstid på minst et halvt år, oppad begrenset til to år.

I disse gigantiske databasene vil det fremgå hvem du har ringt til, hvor du har ringt fra, når du har ringt og hvor lenge, både via fasttelefon og mobiltelefon. Tilsvarende også hvem som har kontaktet deg. Direktivet krever lagring av informasjon om når du benyttet Internett og med hvilken adresse. Videre skal det loggføres hvem du har sendt e-post til og mottatt e-post fra.

I meldingsåret kom også Avinors planer om å prøve ut kroppskanning på norske flyplasser. Forslaget føyde seg etter Datatilsynets mening inn i rekken av stadig mer integritetskrenkende tiltak. Avinor besluttet etter massive protester å legge prosjektet på is.

I noen tilfeller tilbyr produsenter av ny teknologi sterkt reduserte priser for å få sin teknologi inn i prestisjeprosjekter. Med dette oppnår de å få et utstillingsvindu for sitt konsept, og samtidig skape legitimitet for sine løsninger.

Innføringen av mange integritetskrenkende tiltak er ikke tuftet på tilstrekkelige avveininger. Flere ser mer ut som resultatet av en sterk lyst til å være innovativ, koblet med en iver etter å vise handlekraft.

Datatilsynet etterlyser en tilsvarende iver og handlekraft når det gjelder å evaluere de integritetskrenkende tiltakene som allerede er innført.

9 Nærmere om utvalgte saksfelter

9.1 Justissektoren

9.1.1 Tiltak mot hvitvasking og terrorfinansiering

Finansdepartementet sendte i meldingsåret et forslag til revisjon av hvitvaskingsloven til høring (NOU 2007:10). Forslaget skal implementere det tredje hvitvaskingsdirektivet, og er utarbeidet av et utvalg hvis mandat blant annet var å vurdere hvordan "..hensynet til personvern kan ivaretas på en hensiktsmessig måte." Etter Datatilsynets mening har ikke utvalget gjennomført dette.

Fem fundamentale spørsmål er etter tilsynets mening ubesvarte i lovendringsforslaget:

1) Nytteverdien av den eksisterende rapporteringsplikten er ikke dokumentert.
Økokrim har de siste fem årene mottatt hele 22 767 rapporter om mistenkelige transaksjoner. Antallet ser ikke ut til å avta. Kun et fåtall av de innmeldte transaksjonene ender med domfellelse, men bruken av meldingene ser ut til å være nyttige for andre aktører, og for andre formål. Datatilsynets bekymring er primært rettet mot alle de uskyldige som åpenbart er innmeldt til Økokrim. Utviklingen i forhold til finansinstitusjoners meldeplikt går i retning av at man heller rapporterer én for mye enn én for lite, da brudd på meldeplikten er straffesanksjonert.

2) Manglende behovsanalyse – trenger man de foreslåtte endringene?
Utvalget har ikke dokumentert hvilke kriminalitetstyper som ikke oppklares ved de eksisterende reglene. Ett av forslagne går likevel ut på å senke terskelen for overtredelse av reglene om lovpålagt rapportering til også å omfatte grov uaktsomhet. En beskrivelse av trusselbildet og de reelle behovene er helt nødvendig for at høringsinstanser og lovgiver skal kunne ta stilling til om tiltakene er nødvendige og forholdsmessige.

3) Hvor langt skal samfunnet tillate privat etterforskning?
Helt nytt i lovforslaget er at rapporteringspliktige skal underlegges en plikt til å foreta omfattende kundekontroll. I tillegg er det stilt krav om forsterkede kontrolltiltak overfor politisk eksponerte personer og deres krets. Datatilsynet er kritisk til at sivile samfunnsinstitusjoner pålegges en plikt til å kartlegge sensitive forhold rundt kunden. Forslaget innebærer et enda tettere institusjonalisert samarbeid mellom sivile samfunnsinstitusjoner og politiet. Spørsmålet om hvor lange politiets forlengende armer skal være fortjener en prinsipiell politisk debatt.

4) Hvilke konsekvenser har det at viktige rettssikkerhetsgarantier oppheves?
Datatilsynet konstaterer at det nye lov- og forskriftsforslaget vil føre til større grad av hemmelighold overfor den innrapporterte enn tidligere. I kombinasjon med en utvidet undersøkelsesplikt for den rapporteringspliktige, bidrar dette til en betydelig svekket mulighet for den enkelte til å få vite hva andre vet om ham eller henne. Hemmelighold er med på å svekke den grunnleggende tilliten mellom individ og myndigheter, som igjen er en grunnleggende forutsetning for et velfungerende og vitalt demokrati.

I saker som angår kommunikasjonskontroll, har den kontrollerte i ettertid anledning til å gjøre seg kjent med omfanget av kontrollen. En tilsvarende rettighet bør innrømmes personer som blir innrapportert i henhold til hvitvaskingsloven.

Datatilsynet vil heller ikke utelukke at en større grad av åpenhet hva gjelder innhenting, utlevering, bruk og videreformidling av opplysninger også vil kunne ha en preventiv effekt. Vissheten om at noen "ser en i kortene" kan kanskje bidra til at man avstår fra videre kriminell virksomhet.

5) Hvilken rolle skal Kontrollutvalget ha?
Det samlede lov- og forskriftsforslaget representerer såpass store innhugg i personvernet at Kontrollutvalgets rolle burde vært drøftet i utredningen. Når innsynsmulighetene mangler, bør kanskje Kontrollutvalgets rapporter, funn og møtereferater, dersom slike eksisterer, være offentlig tilgengelige i en eller annen form.

9.1.2 Datakrim

Datakrimutvalgets delrapport II ble sendt på høring i meldingsåret. Datatilsynet anerkjenner at nye former for kriminalitet krever nye straffebestemmelser og nye måter å etterforske lovbrudd på. Tilsynet hadde i sin høringsuttalelse likevel innvendinger, blant annet at forslaget er språklig vanskelig tilgjengelig.

Beskrivelsene av de straffbare handlingene er svært runde og vide, men følges av omfattende skjønnsmessige begrensninger. Disse viser gjerne til noe ”utenfor seg selv”, for eksempel normer, etikk, retningslinjer osv. Begrepet uberettiget er brukt i nesten alle bestemmelsene i lovforslaget, og gjør dem vanskelig å tolke. For eksempel: ”For uberettiget bruk straffes den som uberettiget benytter andres datasystem eller elektroniske kommunikasjonsnett”.

Datatilsynet mener at skjønnsmessige begrep må defineres nærmere slik at både befolkning og rettsapparat kan ha klare ideer om hva man skal forholde seg til. Det kan bli vanskelig å vite når man er på rett og gal side av loven. De følgende bestemmelsene viser til ”uberettiget” befatning med diverse verktøy og koder. Hvem klarer, på fornuftig vis, enkelt å forklare hvilken handling som kan utløse straffeansvar etter bestemmelsene under?

> *§ 10 Ulovlig befatning med tilgangsdata*
>
> *For ulovlig befatning med tilgangsdata straffes den som uberettiget anskaffer, innfører, fremstiller, besitter, markedsfører eller tilgjengeliggjør for andre passord, adgangskode, krypteringsnøkkel eller lignende som kan gi tilgang til data, databasert informasjon eller datasystem.*
>
> *Straffen er bøter eller fengsel i 1 år. For grov overtredelse er straffen bøter eller fengsel inntil 3 år.*
>
> *§ 11 Skadelig dataprogram og utstyr*
>
> *For ulovlig befatning med skadelig dataprogram straffes den som uberettiget anskaffer, fremstiller, modifiserer, besitter, markedsfører eller tilgjengeliggjør dataprogram som er særlig egnet til å begå handlinger som er straffbare etter §§ 4-8, 10 eller 13-14 i dette kapitlet. Liknende befatning med utstyr som er særlig egnet til tilsvarende formål straffes på samme måte.*
>
> *Straffen er bøter eller fengsel inntil 1 år. For grov overtredelse er straffen bøter eller fengsel inntil 3 år.*

Datatilsynet er bekymret for at bestemmelsene, slik de er formulert, kan få et for vidt nedslagsfelt. Som mindretallet i utvalget pekte på, er det normalt ikke straffbart å besitte gjenstander som kan benyttes til kriminelle formål, for eksempel en eske fyrstikker eller et brekkjern. Mindretallets anførsel om at dataprogrammer som har et skadepotensial og brukes til straffbare forhold også kan benyttes til lovlige og nyttige formål, bør tillegges betydelig vekt.

Datatilsynet er generelt kritisk til å kriminalisere handlinger som ikke i seg selv krenker noen beskyttelsesverdig interesse. Bestemmelsene innebærer en uheldig dreining mot økt subjektivisering av strafferetten, noe som igjen kan lede til et økt kontrollnivå i samfunnet.

Bruk av fiktiv identitet

Bruk av fiktiv identitet er noe barn og unge oppfordres til av flere samfunnsinstitusjoner, også av Datatilsynet. Se for eksempel nettstedet www.dubestemmer.no. Hensynet bak denne oppfordringen er at barn og unge bedre skal kunne beskytte seg mot uønskede og straffbare handlinger. Lovforslaget vil kunne bidra til betydelig usikkerhet knyttet til bruk av pseudonymer eller kallenavn

Datatilsynet er klar over at det kan forekomme krenkende handlinger ved bruk av uriktig identitet. Imidlertid er bruken av uriktig identitet utbredt, og bør i mange sammenhenger anses som legitim. Å oppgi uriktig identitet kan eventuelt vurderes som straffeskjerpende i kombinasjon med annen kriminell handling, men bør ikke være en ulovlig og straffbar handling i seg selv.

Filtrering

Et mindretall foreslo at tjenesteytere skal kunne pålegges å blokkere tilgangen til bestemte steder på Internett for sine brukere dersom innholdet vil kunne medføre straffeansvar i Norge. Datatilsynet støtter ikke forslaget. Spørsmål om filtrering er et meget ømtålig tema som eventuelt først må bli gjenstand for en bred konsekvensanalyse. – Hvem skal bestemme hva som skal blokkeres? spurte Datatilsynet i høringsuttalelsen, og påpekte at det vil det være høyst ulike meninger om slike spørsmål i et demokrati.

9.1.3 Skal pressen og forskere kunne følge politiet under arbeid?

Justisdepartementet sendte ut et forslag om at andre enn de som utfører tjeneste eller arbeid for politiet skal kunne gis tillatelse til å følge og observere politiets tjenesteutøvelse på privat og offentlig sted. To samfunnsaktører ble vurdert spesielt, nemlig forskere og pressemedarbeidere.

Disse to samfunnsaktørene er vidt forskjellige både med hensyn til hvilke interesser de representerer og hvilken rettslig regulering de er underlagt. Datatilsynet støtter ikke forslaget om å tillate pressemedarbeidere å følge og observere politiets tjenesteutøvelse på privat sted.

Pressen er ikke er underlagt alle de begrensninger i forhold til taushetsplikt og andre bestemmelser som skal ivareta den enkeltes personvern. Heller ikke personopplysningsloven vil komme til anvendelse dersom pressen behandler opplysningene i strid med formålet, da loven, i det vesentligste, ikke gjelder behandling av personopplysninger for journalistiske formål.

Stor og uopprettelig skade vil kunne skje dersom pressen publiserer personopplysninger som resultat av observasjon av politiets tjenesteutøvelse. En ”smekk på fingrene” fra PFU i ettertid vil ikke kunne reparere en slik skade, da skaden inntreffer i og med publiseringen.

Verken journalist eller pressemedarbeider er en beskyttet tittel. Dette vil i praksis kunne skape problemer med å avgrense hvilke aktører som skal kunne gis tillatelse.

En tillatelse til at forskere skal kunne følge og observere politiets tjenesteutøvelse er mindre betenkelig.

9.1.4 Tilsyn i fengselsvesenet – Ila fengsel

Datatilsynet rettet skarp kritikk mot Justis- og politidepartementet, etter å ha gjennomført en kontroll med den behandling av sensitive personopplysninger som skjer i fengselsvesenet. De alvorlige lovbruddene som er avdekket viser at personvernet til mer enn 30 000 tidligere innsatte og deres pårørende ikke er ivaretatt.

Datatilsynet har over flere år mottatt klager fra innsatte ved landets fengsler, knyttet til behandling av personopplysninger i fengslene. Særlig har det vært klaget på at opplysningene om fangene og deres pårørende ikke er tilstrekkelig beskyttet. Datatilsynet sendte spørsmål om håndteringen av opplysningene til Justis- og politidepartementets kriminalomsorgsavdeling. Under korrespondansen fremkom opplysninger som etter tilsynets vurdering ga grunnlag for å foreta en nærmere kontroll. Datatilsynet dro på tilsyn til Ila fengsel høsten 2007.

Datatilsynet konkluderte med at det foreligger et uoffisielt og ukontrollert personregister ved Ila (”innsatt per nummer”). Registeret inneholder svært sensitive personopplysninger. I tillegg mangler bruken av personopplysninger i fagsystemet Kompis et rettslig grunnlag.

De registrertes grunnleggende rettigheter etter personopplysningsloven, med hensyn til innsyn, retting og sletting, blir ikke ivaretatt.

I tillegg påpekte Datatilsynet at Kriminalomsorgsavdelingen ikke har etablert et internkontrollsystem for å sikre at behandlingen av personopplysninger skjer i henhold til lovgivningen, ikke har foretatt relevante risikovurderinger av behandlingen, eller sørget for tilfredsstillende informasjonssikkerhet, særlig med tanke på konfidensialitet.

Datatilsynet mener også at Justisdepartementets kriminalomsorgsavdeling har gitt tilsynet mangelfull og feilaktig informasjon på vesentlige punkter.

Har en innsatt rett til et personvern?

Ved første øyekast er det ikke innlysende at en som sitter i fengsel har rett til et personvern. Hele formålet med fengselsoppholdet er jo nettopp frihetsberøvelse, gjennom en kontinuerlig personkontroll. Den som sitter fengslet har da heller ikke et tradisjonelt privatliv. Avhengig av de konkrete soningsvilkårene vil privatlivet være kraftig beskåret, med blant annet ransaking av celle og kontroll av postsendinger.

Personvern er en menneskerettighet. Den er nedfelt i den europeiske menneskerettighetskonvensjon (EMK) artikkel 8, som Norge har forpliktet seg til å etterleve. Også Grunnloven har bestemmelser som innebærer at borgerne har en grunnleggende rett til personvern. EMK gir staten på visse vilkår anledning til å straffe enkeltmennesker, gjennom berøvelse av individuelle friheter. Disse kan likevel ikke settes

til side i større grad enn nødvendig for å gjennomføre soningen. Fanger har altså rett til personvern, herunder respekt for den eventuelle rest som er igjen av et privatliv i fengselet.

Særlig viktig er det at opplysninger om at en person sitter eller har sittet i fengsel, og de nærmere omstendighetene rundt dette, behandles konfidensielt. Det er helt nødvendig for blant annet å sikre at den innsatte har reelle muligheter til å føres tilbake til samfunnet. Og nettopp det å gjøre den innsatte i stand til å føre et fullverdig liv utenfor murene er jo et av straffens hovedformål.

Videre er det viktig at de personene som opplysningene gjelder (herunder pårørende), får tilstrekkelig informasjon til å kunne ivareta sine øvrige rettigheter, blant annet rett til innsyn i opplysningene.

9.1.5 Overføring av passasjeropplysninger til USA

Etter terrorangrepene i 2001 har USAs myndigheter krevd en rekke opplysninger om flypassasjerer som kommer inn i amerikansk luftrom. I meldingsåret ble en ny avtale om overføring av passasjerdata undertegnet av EU og USA. Kravet om personopplysninger omfatter passasjerenes navn, kontaktopplysninger, reiserute, reisefølge og eventuell diett, og en rekke andre opplysninger.

Den nye avtalen mellom USA og EU om overføring av flypassasjerdata gir betydelig svekket personvern, uttalte Artikkel 29-gruppen, et offisielt rådgivende personvernorgan i EU, da de behandlet avtalen.

Avtalen legger opp til at en enda større mengde opplysninger skal kunne overføres. Formål, beskyttelse og personverngarantier i avtalen er ikke presist formulert, og åpner for mange unntak. Lagringstiden er økt til minst 15 år. Det er blant annet ikke lenger noe krav til sikkerhetsnivået ved videre overføring fra Department of Home Security (DHS) til andre kontorer innen USA eller i utlandet.

Overgangen fra en tilstand der USA forsyner seg selv i reiseselskapenes registre, til en tilstand der reiseselskapene sender opplysningene på forespørsel, er uavklart på flere punkter, påpekte Artikkel 29-gruppen videre. Blant annet er det ikke åpenbart hvordan DHS, som i unntakstilfeller skal få anledning til å hente ut andre opplysningene av registeret enn de som er ramset opp i avtalen, skal kunne få tak i disse opplysningene når de ikke lenger får forsyne seg selv hos reiseselskapene.

Artikkel 29-gruppen reagerte også på at ingen uavhengige tilsynsmyndigheter er tiltenkt rollen som kontrollør.

Artikkel 29-gruppen ba Kommisjonen klargjøre flere punkter, blant annet:

- Hvilke flyselskap er omfattet av avtalen?
- Når kan dataene bli brukt til andre formål enn avtalens hovedregler tilsier?
- Hvordan skal opplysningene kunne hentes ut etter unntaksregelen, uten å gjeninnføre prinsippet om at amerikanske myndigheter forsyner seg selv i flyselskapenes databaser?
- Hvilke 13 flyselskaper overfører data i dag, og hvilke krav de må oppfylle?
- Når vil tilsyn finne sted?

I tillegg ønsket gruppen forsikringer om at tidsfristen for opphør av at "selvforsyning", 1. januar 2008, ikke blir skjøvet på flere ganger.

Norge er ikke omfattet

Norge er ikke omfattet av den nye avtalen når denne årsmeldingen leveres til Fornyings- og administrasjonsdepartementet. For at et flyselskap lovlig skal kunne utlevere passasjerinformasjonen fra Norge, må det innhente samtykke fra passasjeren, eller søke Datatilsynet om dispensasjon fra forbudet mot å utlevere personopplysninger til stater som ikke sikrer et tilstrekkelig beskyttelsesnivå. Justisdepartementet og Utenriksdepartementet arbeider med å få til en avtale mellom USA og Norge.

Datatilsynet legger stor vekt på at passasjerene får informasjon før billettkjøpet, slik at han eller hun vet hvilke forutsetninger som ligger til grunn for reisen.

9.2 Datalagringsdirektivet

I 2007 har Samferdselsdepartementet forberedt høringen for implementeringen av datalagringsdirektivet i Norge. Direktivet ble vedtatt i EU i 2006, og skal implementeres i EU-landene senest innen starten av 2009. Norge har ikke hatt mulighet til å påvirke innholdet.

Datatilsynet har vært opptatt av å få frem at direktivet er et helt nytt verktøy for myndighetenes overvåking av innbyggernes elektroniske kommunikasjon. I fjorårets årsmelding påpekte Datatilsynet at innføringen av datalagringsdirektivet er et paradigmeskifte i det norske rettssystemet. Med dette direktivet innfører man et etterforskningsmiddel som omfatter hele befolkningen. Det er et breddetiltak, ikke målrettet mot enkeltpersoner eller grupper av personer det hefter en mistanke ved.

Hittil har det vært nødvendig å ha et klart behandlingsgrunnlag for å lagre trafikkdata om innbyggernes kommunikasjon. Teleoperatørene har lagret trafikkdata for å kunne fakturere kunder i ettertid. De kommunikasjonsmetodene som ikke er basert på fakturering av forbruk, har det ikke blitt lagret trafikkdata for. Direktivet krever at trafikkdata for fasttelefon, mobiltelefon, bredbåndstelefoni, e-post og internettilgang, skal lagres. For enkelte tjenester innen telefoni har det i Norge vært lagret trafikkdata i tre til fem måneder. For e-post og internettilgang har det ikke vært vanlig å lagre trafikkdata.

Direktivet krever lagring i fra seks måneder til to år. Mange europeiske land legger seg på ett års lagring. Det er antydet at Tyskland vil velge kortest mulig lagring, seks måneder.

Lagringen er detaljert. Når det for eksempel gjelder e-post, hvor det ikke er blitt foretatt trafikkdatalagring tidligere, skal det nå lagres hvem du sender e-post til og hvem du mottar e-post fra. Videre skal det lagres tidspunkt for e-postforsendelsen og hvilken IP-adresse du benytter. Når det gjelder mobiltelefon, vil lokaliseringsopplysninger bli lagret, i motsetning til før.

Direktivet krever ikke lagring av innholdet i meldingene. Datatilsynet spør imidlertid om man, når man legger opp til en så radikal omlegging av tidligere prinsipper, vil stoppe med dette.

En rekke fagfolk har påpekt at det er uklart hvordan direktivet skal forstås. Er det bare politiet som skal få tilgang, eller skal andre, som tollvesenet, skattevesenet eller liknende

etater også få tilgang? Direktivet legger opp til at hvert enkelt land selv må avklare en rekke parametere. Det har vært mye diskusjon rundt hva som skjer dersom noen land velger seks måneders lagringstid, mens andre velger to år.

Datatilsynet er bekymret for at all uklarheten rundt direktivet vil føre til en ukontrollert overvåking av den enkelte.

9.3 Telefoni

9.3.1 Omfattende lekkasjer fra teleselskapene – anmeldelse

Nettstedene til flere teleselskaper ble brukt til innhøsting av personopplysninger i perioden 28. juli til ca. 7. august 2007. Datatilsynet hadde i lang tid fryktet slike hendelser på grunn av måten flere kundesider var konstruert på. Tilsynet var også kritisk til at flere aktører bare krevde å få oppgitt fødselsnummer når de skulle identifisere personer ved etablering av et nytt kundeforhold. Datatilsynet tok opp spørsmålet med flere av aktørene første gang høsten 2006, uten å møte stor forståelse for tematikken.

Datatilsynet kontrollerte en rekke virksomheter, mens andre mottok brev fra tilsynet med oppfordring om å sørge for at deres systemer ikke hadde denne svakheten.

Innhøstingen av personopplysninger startet med en liste fødselsnumre laget av et dataprogram. Disse ble senere sjekket mot en offentlig nettside for å luke ut numre som ikke er i bruk. Fødselsnumrene ble videre benyttet til å søke frem enkeltpersoners navn og adresse via teleoperatørenes nettsider. Få av personene som ble rammet hadde noe med virksomhetene å gjøre, og svært mange ble opprørt og overrasket over at dette rammet nettopp dem.

Datatilsynet var kritisk til følgende punkter:

1. Teleselskapenes nettsteder tillot enhver å bestille abonnement kun ved å oppgi fødselsnummeret til et individ. Virksomheten sikret ikke at kommunikasjon skjedde med rette vedkommende.
2. Nettsiden føyde til navn, adresse og hvorvidt innehaver av fødselsnummer var kredittverdig eller ikke. Dermed ga selskapene innsyn i personopplysninger uten at de med rimelighet hadde forvisset seg om at dette skjedde til rette vedkommende. I realiteten brukte de fødselsnummeret som et slags ”legitimasjonsbevis”.
3. At virksomhetene ikke på selvstendig initiativ sikret informasjon forsvarlig.
4. Flere av virksomhetene oppfylte ikke meldeplikten til tilsynet etter personopplysningsforskriftens § 2-6, men først ga underretning etter krav fra tilsynsmyndigheten.
5. Flere av virksomhetene tok seg ikke bryet med å varsle berørte ofre.

Datatilsynet mener at de klart alvorligste krenkelsene ligger i mangelfull sikring av informasjon, respons med tilleggsinformasjon og at flere virksomheter ikke tok seg bryet med å varsle ofrene for hendelsen. Manglende varsling av berørte vitner om en manglende respekt for personvernet til den enkelte.

Ikke alle de ovennevnte regelverksbruddene er straffesanksjonert. Datatilsynet valgte å anmelde brudd på personopplysningslovens § 13 om informasjonssikkerhet, og personopplysningsforskriftens § 2-6 om varslingsplikt overfor tilsynet. Det var kun virksomheten Talkmore AS som oppfylte begge kriteriene, og som dermed ble anmeldt.

I vurderingene som ble foretatt, avdekket Datatilsynet svakheter i regelverket. Terskelen for straffereaksjoner i forhold til denne typen saker er høy. Bruk av overtredelsesgebyr hadde trolig vært langt mer egnet enn anmeldelse. Etter gjeldende lovverk har imidlertid ikke Datatilsynet slike virkemidler.

9.3.2 Tilsyn hos to teleoperatører

Datatilsynet besøkte to teleoperatører høsten 2007. Begge de kontrollerte virksomhetene hadde en utilfredstillende sikring av trafikkdata for kundene. For mange ansatte hadde tilgang til denne type data, og kontrollmekanismer, som for eksempel bruk av logger, var fraværende. Et annet fellestrekk var brudd på sletteplikten etter personopplysningslovens § 28.

Behandlingen av personopplysninger i telebransjen er konsesjonspliktig. En av virksomhetene hadde ikke konsesjon fra tilsynet. Den andre virksomheten hadde konsesjon, men brøt konsesjonsvilkårene på det aktuelle tidspunkt, ved at lagringstiden overskred den maksimale lagringstiden med god margin. Begge brøt informasjonsplikten, og fikk anmerkninger for en ikke tilfredsstillende internkontroll.

Det gjennomførte tilsynet styrket Datatilsynets bekymring i forhold til en eventuell innføring av datalagringsdirektivet. Teleoperatørene synes ikke å ha utviklet en forståelse av at trafikkdataene de håndterer er videre beskyttelsesverdige. Dette mener tilsynet å kunne slå fast basert på synspunktene virksomhetene ga under kontrollen, funnene som ble gjort og tidsrommet bruddene åpenbart har pågått i.

9.3.3 Pliktig registrering av telefonbrukere, ikke bare av abonnentene

Samferdselsdepartementet har i løpet av året 2007 fremmet et forskriftsforslag om at ikke bare mobilabonnentene skal registreres, men også den som faktisk bruker mobilen. Abonnent og bruker er ikke nødvendigvis samme person. Norge har allerede gått betydelig lengre enn andre europeiske land. Anonyme abonnementer på mobiltelefoner kan ikke lenger opprettes i Norge. I Sverige kan man fortsatt være anonym.

Det virker som at hovedargumentet for å innføre registreringen av identitet er å fange opp brukere under 18 år. De mindreårige skal dermed kunne beskyttes fra å få reklame, eller andre henvendelser som ikke egner seg for dem.

Datatilsynet mener det er unødvendig å foreta en full registrering av brukerne av mobiler for å forhindre dette. Det er i tillegg åpenbart at også mange personer *over* 18 år helst vil slippe denne typen henvendelser.

Datatilsynet er spesielt bekymret for pliktig registrering av brukere under 18 år. Mange foreldre velger å la mobiltelefonene stå i eget navn, nettopp for å beskytte barna. Det som er tenkt å beskytte barna mot uønsket reklame kan gjøre dem sårbare for henvendelser fra

personer som ikke vil dem vel. Registreringen av brukeren har i flere tilfeller ført til at barn, uten de foresattes viten, er blitt oppført med fullt navn og mobilnummer på nummeropplysningstjenester. Sikkerheten for barnet har dermed ikke blitt bedret.

9.4 Internett

9.4.1 Tilsyn: Det offentliges nettsteder

Datatilsynet førte tilsyn med et begrenset antall nettesteder innen offentlig sektor. Sektoren ønsker å tilrettelegge for økt tilgjengelighet og interaksjon med publikum. Dermed har det blant annet blitt lagt opp til innsending av elektroniske skjemaer.

Slik bruk av Internett krever god sikkerhetskultur og ryddig håndtering av brukernes rettigheter til bl.a. formålsmessig lagring, sletting, informasjon og innsyn. Datatilsynet vurderte hjemmesidene til virksomhetene, og avdekket flere, omfattende og systematiske mangler når det gjaldt informasjon til den enkelte, sikkerhet og forsvarlige rutiner.

Det kom i løpet av tilsynene frem at svært mange kommuner benytter en ekstern leverandør til å ta i mot søknader. Det var ikke laget tilfredsstillende avtaler for dette. Den eksterne leverandøren lagret kopier av alt som ble innsendt via tjenesten. Ansatte hos den eksterne leverandrøren hadde full tilgang til å lese søknader sendt til rundt 160 norske kommuner over en periode på mer enn ett år.

Datatilsynet er bekymret for at svært mange offentlige aktører har lav bevissthet rundt personvernspørsmål og informasjonssikkerhet i tilknytning til nettstedene sine.

9.4.2 Ny offentlighetslov

Forslaget til forskrift til den nye offentlighetsloven pålegger en rekke organer og etater å gjøre den elektroniske postjournalen tilgjengelig på Internett.

Dette medfører behov for klare regler om hva som kan publiseres og kontrollrutiner for å forhindre menneskelige feil og systemsvikt.

Datatilsynet peker spesielt på fire behov:

1) Skjerming av flere opplysningstyper, som trivielle personopplysninger, fødselsnumre og elevlister.
2) Begrensinger med hensyn til hvilke søk man kan foreta.
3) Begrensninger i muligheten til å høste journaler og dokumenter i store mengder.
4) Sanksjonsmuligheter.

Om det offentlige publiserer store mengder trivielle opplysninger om den enkelte, vil det føre med seg en fare for misbruk. Masseinnhøsting av personopplysninger kan gi omfattende profiler av den enkelte. Disse kan blant annet bli tatt i bruk til markedsføring, men også være nyttig for ID-tyveri. Den som ønsker å stjele en identitet kan skaffe seg en tilnærmet fullstendig oversikt over et enkelt individs handlinger og preferanser. Dermed kan det også bli vanskeligere å avsløre en person som fremstår med falsk identitet. Svarene på spørsmål som tidligere var egnet til å skille rett person fra falsk, vil kunne ligge tilgjengelig på Internett.

Datatilsynet har sett en rekke eksempler på at kommuner har publisert personopplysninger som ikke skulle ha vært tilgjengelige på Internett. Noen av dokumentene har inneholdt opplysninger om fødselsnummer, andre er fra enkeltmennesker i krise som har søkt hjelp fra kommunen, andre har vært fullstendige jobbsøknader med skannede attester og vitnemål. Når glippen er et faktum, kan konsekvensene være store for den det gjelder.

Etater og kommuner som opplever at taushetsbelagte personopplysninger publiseres, begrunner gjerne hendelsen med at det er skjedd en menneskelig feil. Datatilsynet mener imidlertid at gjentatte "glipper" tyder på systemsvikt hos virksomheten. Det kan være at det foreligger for dårlige rutiner for gjennomgang av dokumenter før publisering, eventuelt i kombinasjon med at rutinene ikke følges. Rutiner og praksis er et ledelsesansvar, og det er for enkelt når offentlige organer til stadighet skyver sine ansatte foran seg og viser til deres menneskelige feil. Datatilsynet ber derfor i høringsuttalelsen om at man gir en mulighet til å sanksjonere brudd på bestemmelsene.

Vern mot eksponering via søkemotorer

Ikke alle offentlige instanser verner personopplysningene i Internett-publiserte dokumenter mot direktesøk gjennom søkemotorer. Et vern innebærer at en først må klikke seg frem til det aktuelle forvaltningsområdet, og så søke derfra. Mange av sakene som blir behandlet i offentlig sektor gjelder enkeltpersoner. Saksinformasjon som gjelder en privatperson kan dermed lett komme til å dukke opp når en søker på Internett, kanskje med helt andre søkekriterier, og helt andre mål for søkingen. Det er ikke målet med offentlighetsloven at personopplysninger skal pådyttes den som ikke ønsker informasjonen.

9.4.3 Tilsyn: Postlister på nettet

I mai 2007 ble det gjennomført en kontroll hos Ålesund kommune. Bakgrunnen var at Datatilsynet gjennom media ble gjort kjent med et sikkerhetsbrudd. Via søk i søkermotoren Google på Internett var det mulig å finne frem til personer som hadde klaget til Klagenemnda for sosialsaker i 2005.

Kommunens utlegging av sensitive personopplysninger skyldtes flere uheldige omstendigheter. En begrenset mengde opplysninger om klagesaker ble ført på et lavere sikkerhetsnivå enn disse normalt behandles i kommunen. Denne praksisen ble etter hendelsen avsluttet.

Informasjonen var ikke tilgjengelig direkte fra kommunes hjemmesider. Filene ble imidlertid fanget opp av søkemotorer, og de som søkte på navn eller andre tilgjengelige ord i de store søkemotorene, fikk dermed tilgang.

Datatilsynet påla kommunen å etablere et hinder slik at ikke postjournaler og dokumenter systematisk blir søkbare utenfra, via eksterne søkemotorer.

9.4.4 Datatilsynets råd til regjeringen om e-forvaltning

Fra begynnelsen av 90-tallet begynte det offentlige for alvor å bli interessert i elektronisk samhandling. Man så en mulighet for å utvikle nye, demokratiske kanaler og skape bedre forutsetninger for tjenesteyting fra offentlig sektor. Visjonene var at borgeren i stor grad kunne sitte i sin egne stue, hvor han enkelt kunne sende inn informasjon og motta relevante

tjenester fra det offentlige ved hjelp av noen tastetrykk. De siste årene har løsningene for samhandling begynt å komme.

I et brev til Fornyings- og administrasjonsdepartementet trekker Datatilsynet frem flere punkter tilsynet mener forvaltningen må være spesielt oppmerksom på ved videre utbygging av slike tjenester:

Datatilsynets råd kan oppsummeres slik:

- Ikke bruk fødselsnummer på offentlige portaler,
- vis varsomhet med å knytte sak og person sammen ved publisering av saksdokumenter på Internett, og
- stimuler til økt bruk av e-ID og e-signatur.

Fødselsnummeret er en entydig identifikator, hver person får ett, og samme nummer deles ikke ut til flere enn denne ene. Styrken i nummeret ligger i at det kan brukes til å skille personer fra hverandre, for eksempel i en database, slik at nye opplysninger kan registreres i tilknytning til rett person. En utstrakt bruk av fødselsnummer på Internett vil imidlertid kunne representere en fare for at personopplysninger kommer på avveier. En slik lekkasje fant sted i meldingsåret, dette kan man lese mer om i avsnittet *Datainnhøsting er blitt enklere*.

Mengden personopplysninger som blir publisert i portaler og på offentlige nettsteder kan over tid bli så omfattende og lett tilgjengelig at profiler på enkeltindivider kan få kommersiell verdi. Det er viktig å peke på at også virksomheter utenfor EØS-området kan høste store mengder personinformasjon mot viljen til den enkelte. Da har verken Datatilsynet eller andre europeiske myndigheter muligheter til å håndheve rettighetene i personopplysningsloven eller EU-direktivet.

Datatilsynet tar videre til orde for at regjeringen aktivt skal fremme sikker og trygg samhandling på nettet ved å stimulere til økt bruk av e-ID og e-signatur. Mangelen på slike instrumenter innebærer at det er vanskelig å vite hvem man samhandler med på nettet. Datatilsynet har tatt dette spørsmålet opp med skiftende regjeringer. Saken synes imidlertid ikke å være mindre aktuell i det vi går inn i 2008.

9.4.5 Skattelister på Internett

Som følge av lovendringen Stortinget vedtok våren 2007, kan pressen bestille skattelistene for 2006 elektronisk. Tjenesten er åpen for aviser, magasiner og ukepresse i alle medier. Listene inneholder følgende opplysninger om skattebetalerne; navn, fødselsår, poststed og postnummer, skattekommune, nettoinntekt, nettoformue og utliknet skatt.

Skattedirektoratet understreker at de som mottar listene er ansvarlige for at behandlingen av disse skjer i overensstemmelse med personopplysningslovens krav. Datatilsynet vil i den forbindelse poengtere at journalistisk virksomhet i hovedsak er unntatt fra bestemmelsene i personopplysningsloven. Det er opp til hver enkelt redaktør å definere om egen bruk av opplysningene fra skattelistene faller innunder kategorien journalistisk virksomhet. Datatilsynet har ingen intensjon om å avgjøre hvilken bruk av skattelistene som kan sies å ha en journalistisk verdi. Det ville i så fall være en rolle tilsynet mener er svært problematisk i forhold til viktige grunnprinsipper om en fri, norsk presse.

Da lovendringen ble behandlet, ga Datatilsynet uttrykk for at endringen er uheldig for personvernet. Tilsynet mener det strider mot sentrale personvernprinsipper at opplysninger den enkelte norske borger er pliktig til å levere inn, skal kunne brukes til underholdning, gjøres søkbar eller tilbys for salg i form av SMS-tjenester eller lignende. Det er også betenkelig at offentliggjøringen av skattelistene skjer før fristen for å klage på ligningen har gått ut.

Regjeringens begrunnelse for å gjeninnføre pressens innsyn i skattelistene var blant annet et ønske om å styrke den kritiske debatten rundt skattesystemet. Datatilsynet spør om man, ved langtidspublisering av skattelisteopplysninger, ikke i stedet oppnår en stigmatisering av lavtlønnsgrupper og deres familier. I tillegg ser Datatilsynet at faren for ID-tyveri øker for norske skatteytere når informasjon om den enkeltes finansielle forhold ligger så lett tilgjengelig på Internett.

9.4.6 Fosterforeldre på Internett

Belastende opplysninger om fosterforeldre ble publisert på en bestemt internettside. Nettsiden inneholdt blant annet kommentarer og slengbemerkninger om navngitte fosterforeldres oppførsel, fremferd og utseende. Tilsynet forsto fosterforeldrenes fortvilelse, men vurderte det slik at opplysningene måtte ses på som opinionsdannende, og dermed beskyttet av ytringsfriheten. Datatilsynet understreket at det er en forskjell mellom profesjonelle aktører, som må forventes å tåle mer omtale, og privatpersoner som har åpnet sitt private hjem for å ta imot barnevernsbarn.

Tidligere har Personvernnemnda behandlet spørsmål om lovligheten av publisering av opplysninger om profesjonelle aktører i barnevernssaker på de samme sidene. Dette gjelder blant annet psykologer, barnevernsansatte, politikere, advokater og journalister. Den gangen falt nemnda ned på at bruken av opplysningene var et ledd i opinionsdannende virksomhet. Når bruken av personopplysningene har et utelukkende journalistisk eller opinionsdannende formål, gjelder personopplysningsloven bare i begrenset grad. Det betyr blant annet at man ikke trenger samtykke for å publisere opplysninger om enkeltpersoner.

Norsk Fosterhjemsforening klaget på Datatilsynets avgjørelse, og anførte blant annet at opplysningene er svært sensitive, ofte feilaktige, og at publiseringen er en stor belastning for fosterforeldrene.

Personvernnemnda tok stilling til Internettsiden slik den var på klagetidspunktet. Nemnda er enig med Datatilsynet i at formålet med bruken av opplysninger om fosterforeldrene må ses på som opinionsdannende. Forskjellen mellom de profesjonelle gruppene og fosterforeldrene er etter nemndas mening ikke er så stor at vurderingen bør bli en annen. Nemnda opprettholdt Datatilsynets vedtak.

9.4.7 Tilsyn: nettjenester rettet mot barn og unge

Datatilsynet var på tilsyn hos totalt fem nettjenester med barn og unge som målgruppe. Nettsidenes formål favner vidt, fra rene hjelpetiltak til å tilby kommersielle tjenester. Nettjenestene retter seg mot flere grupper, fra små barn til ungdom og voksne personer.

Nettjenestene hadde til dels store mangler når det gjaldt internkontroll. I to nettsamfunn var kommunikasjonsinnholdet tilgjengelig for den behandlingsansvarlige virksomheten. Dette

ser Datatilsynet som klart integritetskrenkende. Medlemmet vil oppfatte det slik at det han skriver og sier ikke er tilgjengelig for andre enn samtaleparten. I den "analoge" verden er andres tilgang til kommunikasjonsinnhold mellom to samtaleparter strengt regulert. Den samme konfidensialiteten må gjelde når man kommuniserer i en virtuell verden. Det lot til at noen nettjenester oppfatter det som legitimt å lagre kommunikasjonsinnhold for myndighetenes eventuelle fremtidige bruk. Dette er i så fall en svært betenkelig utvikling.

For tjenestene med ideelt formål, hjelp til unge, avdekket kontrollen mangelfull sikkerhet i kommunikasjonen. Dette er alvorlig, fordi tjenesten legger opp til at det kommuniseres sensitive og til dels meget personlige opplysninger.

Manglende overholdelse av meldeplikt og informasjonsplikt var også et tema i flere rapporter. Når nettjenestene til dels informerer dårlig, har mangelfull sikkerhet og dårlig passordbeskyttelse, ligger det til rette for at opplysninger om barn og unge kommer på avveie, eller lettere kan misbrukes.

9.4.8 Når Internett blir en felle for barn

Faremo-rapporten, "Forbygging av internettrelaterte overgrep mot barn", ble lagt frem for Justisdepartementet i januar i meldingsåret. Datatilsynet foreslår i sin høringsuttalelse at Kripos bør få et ansvar for å bistå barn og unge med å fjerne bilder og filmer av seg selv fra Internett.

Dagens barn og ungdommer har flyttet mye av kommunikasjonen og uttestingsarenaene over til Internett. De bruker webkameraer i samtaler de oppfatter som private. De utveksler film-snutter og bilder med mobiltelefonene. De chatter og lager hjemmesider. Barn kan, under sin naturlige uttesting, stå i fare for å produsere noe som samfunnet etterpå vil se på som barneporno.

Når det gjelder bilder som kan karakteriseres som barnepornografi, risikerer ungdommen, eller deres hjelpere, straffeforfølgelse dersom de forsøker å søke frem bildene for å få dem fjernet. Politiet er den eneste instansen som har lov til å søke.

Det viktigste for ofrene vil ofte være å begrense spredningen av materialet. De utsatte barna trenger at noen får et definert ansvar for å få filmene og bildene fjernet, så fort som mulig. Det er en av måtene man kan begrense skaden på.

I meldingsåret ble Datatilsynet kontaktet i forbindelse med en konkret sak der en mindreårig jente ble tatt bilder av, og bildene senere ble publisert på nett. Bildene ville kunne bli tolket som barneporno. Dette satte jenta i en umulig situasjon. Hun kunne ikke søke frem bildene for å få krevd dem slettet, fordi det er straffbart å søke etter barneporno. Hun måtte derimot leve med kunnskapen om at bildene var der, og at de igjen kunne gjøre det vanskelig for henne, uten at hun kunne gjøre noe med saken. Saken fikk store konsekvenser. Jenta måtte bytte navn, familien flyttet, og hun begynte på ny skole.

9.4.9 Tilsyn: Nettsamfunn for voksne

Datatilsynet besøkte to nettsamfunn for voksne høsten 2007. I tillegg ble det gjennomført brevlige/nettbaserte kontroller mot ytterligere seks nettsamfunn. Tidligere tilsyn har avdekket uklarheter i forhold til hvordan tilgang til systemer og applikasjoner skal anordnes. Videre er det i en rekke tilsyn påpekt at behandlingsansvarlig i liten grad sjekker

relevante logger. Dette skaper en situasjon hvor behandlingsansvarlig i begrenset grad har kontroll med hvem som skaffer seg tilgang til personopplysninger.

Nettsamfunn er ”et rom for å kommunisere”. Hensikten med tjenesten er å legge til rette for at brukerne etter eget ønske kan samhandle om det de selv er opptatt av. Virksomheten tilbyr i utgangspunktet en kommunikasjonsplattform og legger begrenset føring på hvordan denne skal brukes. Utover det er det medlemmet selv som bestemmer innholdet i kommunikasjonen.

Nettsamfunnene har såkalte moderatorer som har en slags myndighet i nettsamfunnet. Hos et av nettsamfunnene var moderatorene ansatt i virksomheten som drev nettsamfunnet, mens hos den andre var det frivillige medlemmer av nettsamfunnet. Det var rundt 20 moderatorer hos begge nettsamfunn. Medlemstallet var henholdsvis rundt 250 000 og 550 000.

Datatilsynet mente at virksomhetene ikke ga tilstrekklig informasjon til medlemmene. Blant annet manglet utfyllende informasjon om formålet med behandlingene, opplysninger om i hvilken situasjon utlevering kan bli aktuelt, virksomhetens praksis med hensyn til sletting, prosedyre ved endring av vilkår som berører personvernet mv.

Begge nettsamfunn hadde mangelfull sletting av personopplysninger. Tilsynet påpekte spesielt manglende sletting av klager på andre medlemmer. I disse klagene kunne det fremkomme relativ støtende anklager. Tilsynet påpekte at når disse sakene ble sjekket ut, måtte informasjonen anonymiseres eller slettes.

Begge nettsamfunnene fikk anmerkning for mangelfull sikring av personopplysningene. Anmerkningene gjaldt utilfredstillende beskyttelse av administrasjonstilganger, uklare ansvarsforhold, mangelfull databehandleravtale, manglende tilgangskontroll og mangelfull logging.

9.5 Identifikasjon og legitimasjon

9.5.1 Ikke mindre kontroll med folkeregisteret

Skattedirektoratet sendte i meldingsåret ut et forslag til ny folkeregisterforskrift på høring. Forslaget innebærer svekket kontroll og oppfølging av tilgangen til personopplysningene i folkeregisteret. Folkeregisteret skulle etter forslaget ikke lenger ha en lovmessig plikt til å holde oversikt med hvem som har tilgang til hvilke opplysninger, vilkårene for tilgangen, eller kontroll over at disse vilkårene overholdes.

Tall fra Skattedirektoratets egne hjemmesider viser at i alt 1500 virksomheter hadde tilgang til databasen i folkeregisteret i 2005. Hvert år gjøres omtrent 30 millioner oppslag i denne databasen. Datatilsynet påpekte behovet for en innskjerping snarere enn en lempelse av kontrollen med tilgangen til dette registeret.

Datatilsynet gjennomførte i meldingsåret tilsyn hos flere teleoperatører. Det ble avdekket en rekke omstendigheter som viser behov for tettere kontroll og oppfølging av vilkår og tilgang til denne type opplysninger. Dette mener Datatilsynet i første rekke bør være folkeregisterets eget ansvar.

Datatilsynet påpekte at det er viktig at vilkårene for tilgang til og kontroll av personopplysninger opprettholdes. Personopplysninger som for eksempel fødselsnummer

har vært en viktig råvare for identitetstyverier. Dersom folkeregisterets lovmessige plikt til å holde oversikt over tilgangen til, vilkårene for og kontrollen med opplysningene i databasen faller bort, øker også risikoen for at misbruk ikke fanges opp eller kan etterspores. I og med at det her dreier seg om det sentrale personregisteret i Norge er Datatilsynet opptatt av å jobbe for å beholde en balanse mellom tilgang til og kontrollen av registeret.

Datatilsynet var tilfreds med at tilsynets merknader i høringsrunden ble ivaretatt. I den nye folkregisterforskriftens § 9-2 fremgår det nå at registermyndigheten skal sikre dokumentasjon om hvem som har fått folkeregisteropplysningene, hvilke typer av opplysninger som er utlevert. og de vilkår som er knyttet til vedtaket. I tillegg skal registermyndigheten følge opp om vilkårene blir overholdt.

9.5.2 Utstrakt bruk av fødselsnummer øker risikoen for ID-tyveri

Alle unike identifikatorer vil ha en egenverdi fordi de entydig identifiserer et individ. Unike identifikatorer gjør det mulig å samle informasjon som gjelder en gitt person, slik at man får et mer fullstendig bilde av personen.

Et fødselsnummer utstedes til norske borgere. Et tilsvarende nummer (D-nummer) utstedes til utlendinger som har bo og arbeidstillatelse. Til fødselsnummeret knyttes navn, bosted, alder, eiendomsbesittelse, økonomiske aktiva, sosiale rettigheter mv. De offentlige aktørene benytter først og fremst nummeret til å holde orden på sitt omfattende registerregime. Dersom offentlig sektor betraktes under ett, har man en gigantisk samling av opplysninger om det enkelte individ. Registreringene skjer kontinuerlig fra fødsel til død.

En mer utbredt bruk av fødselsnummer vil føre til at stadig flere aktører får tilgang til en unik nøkkel. Om kobling mellom individ og fødselsnummeret er kjent, vil det i første omgang innebære at noen har tilgang til en unik nøkkel som kan, men ikke nødvendigvis vil, bli brukt. Økt bruk av entydige og varige identifikatorer innebærer en økt risiko for identitetstyveri. Dette henger sammen med at denne felles identifikatoren forenkler tilførsel av nye opplysninger dersom det skulle dukke opp flere kilder.

Tjenestespekteret som tilbys fra offentlig og privat sektor innebærer behov for en kontroll av identitet. Dessverre har ikke arbeidet med e-ID holdt tritt med utviklingen av tjenestespekteret. Det har oppstått et vakuum som fylles med mindre gode løsninger. Flere bruker brukernavn, passord og i noen tilfeller engangskoder eller passordgeneratorer. Slike løsninger kan være tilstrekkelige i forhold til noen formål, men er overhodet ikke egnet i et lengre perspektiv. For det første er det et stort problem at passord gjenbrukes, for det andre at de sjeldent byttes ut og for det tredje at de ikke allment kan trekkes tilbake, da det ikke er forutsatt tredjepartsverifikasjon.

Dersom noen skulle få tilgang til en dårlig sikret base over passord er det dermed stor sjanse for at informasjonen kan misbrukes ovenfor andre virksomheter.

9.5.3 Tilsyn: E-signaturer

Datatilsynet har i løpet av meldingsåret vært på tilsyn hos flere e-ID leverandører. Tilsynene har etterlatt et inntrykk av at feltet ennå er i startfasen, med en betydelig økning i utstedte e-ID'er mot slutten av 2007. Store private aktører som Buypass og Bank-ID har

allerede distribuert et stort antall e-ID'er i befolkningen. Videre står også det offentlige på trappene med sine e-ID løsninger.

Datatilsynet mener at befolkningens gryende tilgang til e-ID'er vil kunne dekke et behov for å kunne identifisere seg i den elektroniske verden. Det er avgjørende viktig for Datatilsynet at de nye e-ID løsningene blir av tilstrekkelig kvalitet også informasjonssikkerhetsmessig. Datatilsynet samarbeider med Post- og teletilsynet på dette feltet, i forbindelse med håndteringen av e-signaturloven.

Det er viktig at brukerne forstår hvor kraftig en e-ID med kvalifisert signatur er. Passord (PIN-koder) og eventuelle kort og andre sikkerhetsmekanismer må håndteres på en måte som gjør at de ikke kan misbrukes av uvedkommende. Det er viktig at e-ID leverandørene gir krystallklar informasjon til brukerne om dette.

Det er imidlertid også viktig at muligheten til å kunne identifisere personer over Internett ikke fører til et krav om at man skal identifisere seg i alle sammenhenger. Datatilsynet kan allerede nå se faren for at aktører fremover vil benytte identifiseringsløsninger uten at det strengt tatt er nødvendig. Datatilsynet vil følge nøye med, nå som befolkningen i større grad får tilgang til elektroniske identiteter, og passe på at unødvendig bruk av e-ID ikke forekommer.

9.5.4 Norsk Tipping

Norsk Tipping har utfordret personvernet på en rekke fronter i meldingsåret. Spillerkortet som tilbys spillerne har en bred funksjonalitet utover det som er nødvendig for å kunne spille Norsk Tipping-spill. Overvåking av spillaktiviteten er også økende.

Spillerkortet kan benyttes for noen av spillene og må benyttes i andre spill, for eksempel for spillene Joker og Extra. Spillerkortet kan, etter en tilleggsprosedyre, brukes til e-signatur. Datatilsynet er opptatt av at Norsk Tippings kunder blir tilstrekkelig informert om hva tippekortet kan brukes til, og at dette er et kort som brukerne må passe på, på lik linje med et bankkort. Datatilsynet har derfor bedt Norsk Tipping om å bedre informasjonen til brukerne.

Datatilsynet har tatt opp sikkerheten ved utstedelse av spillerkortet med Norsk Tipping, Buypass og Post- og teletilsynet. Det foreligger konkrete eksempler på at ID-kontrollen ikke er tilstrekkelig for å forhindre ID-tyveri og misbruk, samt at kunnskapen spillerne sitter inne med er lav.

Datatilsynet har registrert at Norsk Tipping legger opp til full overvåking av spilladferd. Virksomheten vil overvåke hvor mye, hvor fort, og hvor lenge det spilles. Norsk Tipping vil regulere hva som skal kunne tas ut og spilles for i løpet av en time.

Datatilsynet er bekymret for mulighetene for profilbygging.

9.5.5 Fingeravtrykk i pass

Datatilsynet hadde innvendinger mot sikkerheten da de nye passene kom for noen år siden. Passene inneholder biometriske data lagret i en fjernavlesbar brikke. I utgangspunktet ble et ansiktsbilde valgt som biometrisk opplysningstype. Planen er imidlertid å ta i bruk fingeravtrykk også. Datatilsynet mener passene ikke har tilstrekkelig sikkerhetsnivå for den nye, tiltenkte bruken.

Politiet har i slutten av 2007 testet sine nye biometristasjoner hvor blant annet fingeravtrykk innhentes for innplassering i fremtidige pass. Formålet med testene er å sjekke om blant annet kommunikasjonen fra biometristasjonene og til produsenten av pass vil fungere tilfredsstillende.

Justisdepartementet har ennå ikke orientert nærmere om hvordan en eventuell senere innplassering av fingeravtrykk i passene skal håndteres. Datatilsynet er bekymret for informasjonssikkerheten, både i forbindelse med passhåndteringen sentralt, samt hvordan brukerne skal forholde seg til denne typen pass. Et bilde av et fingeravtrykk i et pass vil kunne misbrukes. Det er viktig at tilstrekkelige sikkerhetsmekanismer blir etablert.

Det er fortsatt uklart hva formålet med fingeravtrykkene er, og hvem som skal ha tilgang til denne informasjonen. At denne integritetssensitive informasjonen ligger på en brikke som kan avleses på avstand, gir ekstra grunn til bekymring.

9.5.6 Biometri – bruk av fingeravtrykk

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

Biometri beskrives ofte som ”noe vi er” når det sammenlignes med de tradisjonelle metodene for å gjenkjenne eller bekrefte en persons identitet. De tradisjonelle metodene omfatter ”noe du vet”, for eksempel et passord, og ”noe du har”, for eksempel en kodebrikke. Biometri har sin egenart, det er uløselig knyttet til kroppen vår, på godt og vondt.

De mest kjente formene for biometriske kjennetegn er fingeravtrykk, håndavtrykk og ansiktsform, samt de to øyeteknologiene netthinne- og irisavlesning.

Biometrisk informasjon lagres normalt i form av en såkalt ”template”. Dette er en kodebasert representasjon av materialet, i stedet for å lagre en hel måling, for eksempel et fullt bilde av et fingeravtrykk, med alle dets detaljer. Slike templates brukes blant annet fordi det gjør det lettere å sammenligne avgitt fingeravtrykk opp mot tidligere registrert fingeravtrykk.

Datatilsynets har ikke noe prinsipielt imot bruk av fingeravtrykk eller andre biometriske kjennetegn, men tolker formuleringene i personopplysningslovens § 12 slik at adgangen til bruk er snever. Brukt riktig kan biometri være et godt og effektivt verktøy for sikkerhet. Løsninger som baserer seg på biometri nyter generelt høy tillit i befolkningen, med hensyn til presisjon og sikkerhet. Det er derfor viktig å forhindre uriktig bruk av slike verktøy.

I 2007 mottok Datatilsynet fire vedtak fra Personvernnemnda knyttet til bruk av fingeravtrykk. Sakene gjelder bruk av fingeravtrykk i kombinasjon med ID-kort i adgangskontrollen til Essos tankanlegg, fingeravtrykk som erstatning for medlemskort ved to forskjellige treningssentre, samt bruk av fingeravtrykk i tilknytning til timeregistrering for ansatte i REMA1000. Esso fikk medhold i sitt ønske om å bruke fingeravtrykk under forutsetning av samtykke fra den registrerte. I de øvrige sakene opprettholdt nemnda Datatilsynets avslag. Fra 2006 foreligger i tillegg et vedtak fra Personvernnemnda om at fingeravtrykk kan brukes for kommuneansattes pålogging til datamaskiner med sensitive personopplysninger, dersom den ansatte samtykker.

Personvernnemnda har uttalt at de fem vedtakene om biometri er konkrete, og kun skaper presedens i begrenset grad. Datatilsynet finner likevel at nemnda gjennom vedtakene har sagt en god del om hvordan personopplysningslovens § 12 skal forstås også i andre sammenhenger, og hvor nedre grense for bruk av fingeravtrykk ligger. I begge sakene der bruk av fingeravtrykk ble akseptert har nemnda vist til behovet for sikkerhet. Og i begge sakene er bruken basert på den registrertes samtykke.

På denne bakgrunn har Datatilsynet i meldingsåret omgjort et vedtak som forbød Stortinget å bruke fingeravtrykk i pålogging til datamaskiner, slik at dette nå er tillatt. Stortinget benyttet nøyaktig samme påloggingsløsning som den nemnda vurderte i saken fra 2006.

Datatilsynet har videre besluttet at SAS kan benytte fingeravtrykk i forbindelse med innsjekking av bagasje i selvbetjeningsskranker for å oppnå bedre sikkerhet. Det er en forutsetning for beslutningen at det fortsatt er mulig å sjekke inn bagasje i betjent luke uten å avgi fingeravtrykk, og at den reisende får tilstrekkelig informasjon om løsningen og alternativene.

I meldingsåret ga Datatilsynet veiledning om regelverket til flere produsenter og distributører av fingeravtrykksløsninger. Ingen ting tyder på at sakstilfanget på dette området vil bli mindre i nærmeste fremtid. I tillegg til å håndtere nye saker på feltet, vil Datatilsynet holde et våkent øye med de aktører som lovlig kan benytte fingeravtrykk for å sikre at forutsetningene ikke settes tilside.

9.6 Arbeidsliv

9.6.1 Innsyn i ansattes e-post

I 2007 så Datatilsynet en viss endring i forhold til henvendelser om innsyn i e-post. Det kan synes å ha skjedd en vridning fra konkrete klager fra ansatte som har opplevd innsyn i sin e-postkasse, til at henvendelsene i større grad kommer i forkant av at innsyn gjennomføres, gjennom at virksomheten selv gir Datatilsynet informasjon om sine planer. Datatilsynet ser dette som en bekreftelse på at flere virksomheter nå er kjent med at det finnes grenser for når innsyn i e-post kan gjennomføres, og at det er en del regler og retningslinjer for den faktiske gjennomføringen. Henvendelsene Datatilsynet har mottatt bærer også preg av at virksomhetene ønsker å opptre korrekt og i tråd med de regler som gjelder på området. Når ansatte henvender seg til Datatilsynet, er det i økende grad fordi de faktisk har mottatt informasjon om at innsyn planlegges gjennomført, og at de ønsker en bekreftelse på at fremgangsmåten er i tråd med lover og regler.

Henvendelsene tyder også på at flere virksomheter lager interne regler og instrukser om innsyn i e-post. Samtidig er det ikke til å legge skjul på at innsyn i e-post synes å ha blitt en ”vanlig” prosedyre i en del saker, for eksempel i tiknytning til interne granskninger av forskjellige slag. Datatilsynet har ikke grunnlag for å si at det skjer mer innsyn i e-post nå enn før, men det kan synes som om vi står overfor en økende tendens, uten at dette nødvendigvis har sammenheng med at behovet for innsyn har økt tilsvarende.

Vinmonopolet og Redningsselskapet

Datatilsynet anmeldte i 2005 Vinmonopolet og Redningsselskapet for brudd på personopplysningslovens bestemmelser om informasjonsplikt i forbindelse med innsyn i ansattes e-post. I 2006 ble begge sakene henlagt av påtalemyndigheten. Datatilsynet

påklaget henleggelsene, men de ble opprettholdt av Riksadvokaten. Riksadvokaten anmodet imidlertid om at Statsadvokaten måtte ta stilling til om det skulle foretas videre etterforskning for å avdekke om ansatte i Redningsselskapet hadde tilbakeholdt opplysninger for Datatilsynet. Også denne saken ble henlagt i oktober 2007.

Bazarsaken

Datatilsynet anmeldte i 2006 Bazar Forlag AS for brudd på personopplysningsloven. Anmeldelsen skjedde på bakgrunn av et gjennomført tilsyn med forlaget høsten 2005.

Bakgrunnen for saken var at forlagssjefen i Bazar Forlag AS opprettet en "overvåkingskonto" med navnet backup@bazarforlag.com. Via "overvåkingskontoen" skjedde det en automatisk blindkopiering av inngående e-postkorrespondanse til leder for forlagets kontor i Sverige. Den ansattes personlige e-postkonto var beskyttet med brukernavn og personlig passord.

Forlagssjefen gjorde innsyn i den ansattes inngående e-post gjennom "overvåkingskontoen". Den ansatte som fikk lastet ned og åpnet sin inngående e-post, fikk ingen informasjon vedrørende nedlastingen av e-postene, innsynet i disse, formålet med behandlingen eller eventuell utlevering av informasjonen.

Etter Datatilsynets vurdering brøt Bazar Forlag AS personopplysningslovens bestemmelser på flere punkter, og etter tilsynets vurdering var lovbruddene av alvorlig karakter. Spesielt alvorlig var bruddene på informasjonsplikten etter personopplysningslovens § 19 og § 20.

Politimesteren i Oslo siktet Bazar Forlag AS og forlagssjefen for brudd på informasjonsplikten og ila begge forelegg. Både forlaget og forlagssjefen vedtok forelegget.

9.7 Kameraovervåking

9.7.1 Kameraer i "offentlige pauserom"

Hovedtema for kontrollarbeidet innen kameraovervåking var tilsyn med såkalte "offentlige pauserom", nemlig kafeer, restauranter, barer og utesteder. Disse utgjorde til sammen 11 av de i alt 25 kontrollene.

Barer og utesteder, kafeer og restauranter, har mange likhetstrekk med den funksjonen "pauserommet" har, også selv om det ikke er på arbeidsplassen, og heller ikke direkte innenfor en privat sfære. Folk går til disse stedene for å treffe andre, for å hygge seg, koble av og drive en form for rekreasjon, spise, drikke, feste og danse. Datatilsynet mener man ikke kan vurdere disse stedene på samme måte som man vurderer kameraovervåking av butikker. Verken stedene eller deres funksjon er lik butikkene, og gjestenes personverninteresse vil heller ikke være tilsvarende i de to forskjellige settingene. Mye av den samhandlingen som skjer på barer, restauranter og utesteder har privat karakter – midt i det som også er et offentlig rom. Datatilsynet mener at diskresjonshensyn i noen grad må gjelde. Samtidig må man ta hensyn til kravene som følger av det faktum at barer, utesteder, kafeer og restauranter også er noens arbeidsplass.

Selv om sikkerhet i noen grad skyves foran som et generelt, diffust argument, er de konkrete begrunnelsene i stor grad knyttet til vern av materielle verdier, kanskje særlig svinn av varer og penger. For de steder hvor sikkerhetsproblematikk gjør seg reelt

gjeldende, er trolig dørvakter og interne rutiner det avgjørende for gjestenes og ansattes sikkerhet.

Alle kontrollene førte til varsel om pålegg. Dette gjaldt en rekke forhold, eksempelvis mangelfull varsling og manglende melding. Alle stedene ble varslet om enten opphør av overvåkingen eller innskrenkninger i den eksisterende overvåkingen.

De konkrete vurderingene i forbindelse med kontrollene viser at det er vanskelig å få til en lovlig overvåking av denne typen steder:

1. Det vil normalt ikke foreligge gyldig behandlingsgrunnlag for overvåking av publikumsområdene i lokalet.
2. Overvåking av området rundt bardiskene er vanskelig å få til da det foreligger et todelt personvernhensyn, hensynet til gjestene og de ansatte. Konkret har tilsynet vurdert at overvåkingen ikke er tillatt om den medfører at ansatte blir tilnærmet totalovervåket i sin primære arbeidsstasjon, eksempelvis bak bardisken. Om slik overvåking skal kunne tillates, må det foreligge mer tungveiende hensyn enn svinnproblematikk. Tilsynet har likevel falt ned på at gjestene lovlig kan filmes i det de går inn eller ut av lokalet, der det er et behov for dette.

9.7.2 Tilsyn: Private kan ikke overvåke det offentlige rom

Datatilsynet så i meldingsåret på kameraovervåking i tilknytning til et fotballstadion og overvåking av et større område brukt til næringsvirksomhet. Disse to tilsynene har ett felles tema, kameraovervåking av områder som brukes av allmennheten. Konklusjonene i disse tilsynene viser at private aktører ikke på generell basis kan overvåke det offentlige rom, for eksempel en turvei, selv om veien går over privat grunn.

9.8 Samferdsel - Personvern ved reiser fra A til B

Datatilsynet observerte i 2006 at det ble bygd opp en omfattende infrastruktur for overvåking av reisende, både bilister og innen kollektivtrafikken. Dette dreier seg om alt fra overgripende overvåking med satellitter, overvåking ved hjelp av kameraer og radiofrekvensbrikker (som AutoPASS), til såkalte ”svarte bokser” som sitter i den enkelte bil og registrerer kjøringen. I meldingsåret har denne utviklingen fortsatt. Blant annet er det bestemt at bomringen i Oslo skal bli helautomatisk, det vil si at det ikke lenger skal være mulig å passere bompengeanlegget uten å legge igjen spor.

9.8.1 Bombrikker - AutoPASS

Datatilsynet mottok våren 2007 opplysninger om at alle passeringer i bomstasjonene rutinemessig ble fotografert. Denne informasjonen samsvarte ikke med den offisielle kravspesifikasjonen for AutoPASS, eller de opplysningene tilsynet tidligere hadde mottatt om temaet fra Vegdirektoratet. Det var nemlig bare ugyldige passeringer som skulle fotograferes.

Vegdirektoratet ble bedt om å bekrefte/avkrefte om samtlige passeringer ved bomstasjonene i Norge fotograferes. På bakgrunn av svarbrevet fra Vegdirektoratet, måtte

Datatilsynet konstatere at det tas bilde av alle passeringer, ved alle bomstasjoner. Bildene blir imidlertid bare sendt videre i systemet dersom passeringen er ugyldig, eller ved stikkprøvekontroller. En annen begrensning skal visstnok ligge i at internminnet i kameraet er av begrenset størrelse, og at bildene som ikke videresendes derfor blir overskrevet relativt raskt.

Datatilsynet finner det beklagelig at systemet ikke samsvarer med kravspesifikasjonen, og at verken publikum eller tilsynet har blitt informert om forholdet på et tidligere stadium.

Tilsynet forutsetter at systemet utbedres innen rimelig tid.

De 100 seneste passeringene lagres i AutoPASS-brikken

I begynnelsen av meldingsåret avdekket Datatilsynet det faktum at de seneste 100 passeringene i bomstasjoner en AutoPASS-bruker hadde passert, ble registrert i AutoPASS-brikken. I tillegg ble flere andre passeringspunkter registrert. Verken Statens vegvesen, som systemeier, eller bompengeselskapene hadde informert brukerne om forholdet. Datatilsynet reagerte også på at disse personopplysningene ble lagret på fjernavlesbare brikker, totalt uten konfidensialitetsbeskyttelse.

Datatilsynet mener at Statens Vegvesen har unnlatt å gi utførlig og nødvendig informasjon om lagringen av passeringsopplysninger i AutoPASS-systemet.

Både i Datatilsynet, Personvernnemnda og Samferdselsdepartementet har det vært lagt til grunn at passeringsopplysningene slettes så raskt som mulig etter at faktura er betalt. Det er også lagt til grunn at de som ønsker det, kan inngå en avtale om at opplysningene slettes senest etter 72 timer. Det mest alvorlige er likevel at de ca. en million brukerne av AutoPASS ikke er blitt aktivt informert om at passeringsbrikken på frontruten også er en lagringsenhet som lagrer opplysninger om tid og sted for de 100 seneste passeringene.

Dårlig sikkerhet

I tillegg til lagringen av personopplysninger i AutoPASS-brikken, lagres passeringsopplysninger sentralt. Disse opplysningene er også tilgjengelige for brukerne via diverse påloggingsløsninger. Disse løsningene fremstår også med for dårlig informasjonssikkerhet, med hensyn til konfidensialitet og passordbeskyttelse. Statens vegvesen har i løpet av året 2007 gitt informasjon om at disse systemene skal bedres. Datatilsynet er ikke fornøyd med at dette arbeidet tar lang tid.

I løpet av året 2007 er det en rekke andre virksomheter som ønsker å benytte AutoPASS-systemet, for eksempel til adgangskontroll. I Stavanger ønsker man å benytte AutoPASS-brikken for å gi utvalgte kjøretøyer tilgang til avgrensede områder i byen. Andre private virksomheter har også gitt uttrykk for samme ønske. Økt bruk av AutoPASS-systemet til andre formål enn det opprinnelige, å kreve inn bompenger, gir etter Datatilsynets mening et mindre godt personvern.

9.8.2 Bompasseringer til ligningskontoret

I januar tok Datatilsynet kontakt med Skattedirektoratet om utlevering av bompasseringsopplysninger til kontroll av ligningen. Bakgrunnen for henvendelsen var at en rekke bompengeselskaper hadde fått forespørsler om innsyn fra fylkesskattekontorene.

Datatilsynet ønsket i første omgang en tilbakemelding på hvilket hjemmelgrunnlag Skattedirektoratet legger til grunn for å kreve utlevering av passeringsopplysninger. I tillegg ønsket Datatilsynet en avklaring av hvilke passeringsopplysninger som skal registreres, og hvor lenge de skal lagres av regnskapshensyn.

Per i dag registrerer bompengeselskapene passeringsopplysninger etter retningslinjer gitt av Vegdirektoratet. Skattedirektoratet kan etter ligningsloven kreve innsyn i opplysninger knyttet til konkrete kjøretøy benyttet i næringsvirksomhet. Skattedirektoratet begrunner sitt behov for innhenting av opplysningene med at disse vil kunne belyse påstander i ligningen. Det gjøres likevel klart at skattemyndighetene ikke vil kreve innsyn i opplysninger som skulle ha vært slettet.

I praksis gjøres det i bompengeselskapene ikke noen forskjell mellom lagring av passeringsopplysninger for kjøretøy brukt i næringsvirksomhet eller privat bruk. Datatilsynet advarer mot en situasjon hvor passeringsopplysninger for private kjøretøy oppbevares unødig.

Det er i hovedsak tre ulike betalingsformer tilgjengelig; periodeavtaler, forskuddsbetalte avtaler og etterskuddsbetaling av enkeltpasseringer. Innenfor hver av disse betalingsalternativene praktiseres ulike retningslinjer for sletting av passeringsopplysninger.

Datatilsynet vil ikke nekte bompengeselskapene å oppbevare passeringsopplysninger for kunder som eksplisitt ønsker dette. Det er imidlertid viktig at denne oppbevaringen avtales særskilt med kundene, og at de samtykker aktivt. Kundene må også være innforstått med at skattemyndighetene, og eventuelt andre kontrollmyndigheter, da vil kunne kreve tilgang til de lagrede opplysningene.

Tilsynet er innforstått med at bokføringsreglene er relevante på de fleste områder, og at registrerte opplysninger kan tenkes benyttet til å belyse påstander i ligningen. For tilsynet er det imidlertid viktig å understreke at en overgang fra kontantbetaling til elektroniske betalingsmåter ikke automatisk skaper et behov for langtidsoppbevaring av all detaljinformasjon. For å oppfylle kravet etter bokføringsregelverket skal man kun lagre de detaljene om kjøpet som er nødvendige for å ivareta kravene i dette regelverket.

9.8.3 Tilsyn – Tromskortet, elektronisk billettering

Ordninger med elektronisk billettering er under rask fremvekst i samferdselssektoren. Samferdsel er i stor grad et fylkeskommunalt ansvar, og utviklingen skjer derfor hovedsakelig regionalt. Dette medfører at det vokser frem flere ulike løsninger. Sakene som foreligger viser tydelig mangel på etterlevelse av personopplysningsloven i sektoren. Særlig alvorlig er det at identifiserbare reiseopplysninger registreres og oppbevares på ubestemt tid.

Elektronisk billettering innebærer en trussel for den enkeltes grunnleggende rett til sporfri ferdsel i samfunnet. Datatilsynet mener derfor at det er viktig at de ulike systemene oppfyller kravene i personopplysningsloven. Reiseopplysninger må slettes når det ikke lenger er saklig grunn til å beholde dem.

Datatilsynet fant betydelige mangler. Blant annet manglet et rettslig grunnlag, opplysningene var ikke tenkt slettet i tråd med personopplysningslovens krav,

informasjonsplikten overfor de reisende var ikke oppfylt, og det var uklart om de registrertes rettigheter ble ivaretatt ved behandlingen.

Informasjonssikkerheten var heller ikke tilfredsstillende, blant annet manglet databehandleravtale med driftsleverandør. Det forelå ingen dokumenterte rutiner for å ivareta personopplysningslovens bestemmelser i forbindelse med elektronisk billettering.

9.8.4 eCall

eCall er en planlagt alarmtjeneste for bilulykker i Europa. Tjenesten er tenkt å virke slik at en svart boks i bilen automatisk skal kunne ringe nødnummeret og oppgi bilens posisjon i tilfelle ulykker.

Systemet er planlagt å bli en felleseuropeisk alarmtjeneste for kjøretøy, bygd på alarmnummeret 112. Alle biler som selges i EU-området fra 2010 skal etter planen være utstyrt med satellittposisjonering og kommunikasjon via mobiltelefonnettet. Dette utstyret skal automatisk sende informasjon til nærmeste alarmsentral ved ulykker.

Datatilsynet ser at systemet kan ha visse positive sider, men gjennomføringen vil kunne innebære problemer med hensyn til personvern og beskyttelse av privatlivets fred.

Det foreslåtte eCall-systemet er basert på en nesten øyeblikkelig tale- og dataforbindelse fra en eCall-generator til en offentlig alarmsentral. eCall-henvendelseen utløses automatisk av sensorer i bilen i tilfelle ulykke, eller manuelt av personer som befinner seg i bilen.

eCall-henvendelsen består av to elementer: et 112-oppkall med ren tale (audio) og et minimumsdatasett. Datasettet og talemeldingen overføres via mobilnettet, og behandles som en 112-nødoppringning i mobilnettet. Mobilnettoperatøren legger derfor til opplysninger om abonnentens nummer, og angir posisjonen til oppringeren så presist som mulig. Dette er i tråd med vanlige prosedyrer når noen ringer nødnummeret 112.

Frivillighet

eCall er et overvåkingsinstrument som legger til rette for en massiv registrering. Fra et personvernståsted bør lovlydige bilister ha adgang til å bruke veienettet uten å bli registrert. For Datatilsynet er derfor frivillighet viktig – at hver og en skal ha mulighet til selv å bestemme om bilen skal overvåkes eller ikke.

eCall er ment å være innbygget i kjøretøyet. Det er en felles oppfatning blant datatilsynsmyndighetene i Europa at du selv skal kunne bestemme om boksen skal være aktivert eller ikke. Brukeren, som ikke nødvendigvis er kjøretøyets eier, skal på ethvert tidspunkt ha mulighet til å slå systemet på eller av uten noen form for tekniske eller finansielle hindringer. Denne valgmulighet kunne f.eks. tilbys i form av en bryter eller omskifter, i likhet med den som benyttes i forbindelse med airbags for passasjerer.

Det vil være problematisk for personvernet dersom bilforsikringsselskaper eller bilutleiefirmaer presser sjåføren til å aktivere eCall-systemet. Tilsvarende vil også være situasjonen dersom ansatte som benytter firmabiler, direkte eller indirekte tvinges til å benytte eCall-systemet. Slik tvang vil neppe vil ha rettslig grunnlag i personopplysningsloven.

Posisjonering

Datatilsynet har fått inntrykk av at den foreslåtte eCall-ordningen ikke medfører at bilens posisjon skal følges kontinuerlig av en tredjeperson. Det skal likevel være mulig å fastslå hvor kjøretøyet befinner seg. Boksen skal, etter det som er opplyst, kun få forbindelse med kommunikasjonsnettet hvis det aktiveres i forbindelse med en ulykke eller aktiveres manuelt av en av bilens passasjerer.

I den foreslåtte eCall-ordningen oppbevarer "boksen" data for de tre seneste GPS- /Galileo-registrerte posisjonene, men disse skal ikke kommuniseres med mindre eCall utløses. I så fall vil det være nødvendig å fastsette en klar begrensning av omfanget av de innsamlede dataene. I hvilken grad det i fremtiden vil være mulig å fjernaktivere sporingsverktøyet, er foreløpig mer uklart.

9.8.5 Nakenskanning

Avinor ga høsten 2007 uttrykk for et ønske om å teste en "bodyscanner". Dette en maskin som benytter radiostråling (millimeterbølger) for å se om en person bærer skjulte objekter på kroppen. Strålingen kan ikke "se" objekter under huden. Innretningen "kler deg naken", og representerer uten tvil et betydelig inngrep i den personlige integritet.

Avinor var i dialog med Datatilsynet om tiltaket. I en pressemelding har etaten uttalt at reaksjoner fra ansatte, tilbakemeldinger fra Datatilsynet og reaksjoner i opinionen gjør at uttestingen ikke blir gjennomført som planlagt våren 2008. Avinor ønsker å innhente ytterligere erfaringer, blant annet fra utprøving av utstyret i andre land, før en eventuell videre uttesting.

Avinors planer om å innføre kroppskanning på norske flyplasser føyer seg inn i rekken av stadig mer integritetskrenkende tiltak. Datatilsynet har sett med økende bekymring på hvordan ny teknologi introduseres på en måte som gir lite rom for personvernet. Det er ikke nødvendigvis noe motsetningsforhold mellom bruk av ny teknologi og personvern. Kroppskanningen viser imidlertid hvordan motsetningen mellom sikkerhetsbehov og personvern kan oppstå. Er det virkelig nødvendig med tiltak av denne typen, eller kan tilsvarende trygghet oppnås på mer akseptabel måte?

9.8.6 Elektronisk behandling av reiseopplysninger

Innen luftfarten registreres det store mengder personopplysninger. Opplysningene skal bl.a. leveres ut til offentlige myndigheter i Norge og andre land. Det er vanskelig å få oversikt over hvordan opplysningene flyter i disse store systemene, og når de eventuelt endelig slettes. Informasjonsbehandlingen er i all hovedsak lovpålagt, gjennom ratifisering av internasjonale avtaler på luftfartsområdet.

Det er en trend at flyselskapene oppretter en slags reisekonto, hvor opplysninger om bestilte og gjennomførte reiser oppbevares og gjøres tilgjengelige for kunden på Internett. Opplysningene blir med andre ord ikke slettet. Dette er ansett å være en service overfor kundene, og må etter Datatilsynets vurdering derfor bero på samtykke.

Datatilsynet så spesielt på oppbevaring og tilgjengeliggjøring av reiseopplysninger på den enkeltes "konto" hos ett flyselskap. Funnene er nedslående. Behandlingen mangler rettslig grunnlag. Opplysningene slettes ikke i tråd med personopplysningslovens krav.

Informasjonsplikten overfor de reisende er ikke oppfylt, og det er uklart om de registrertes rettigheter blir ivaretatt ved behandlingen. Heller ikke informasjonssikkerheten er tilfredsstillende, blant annet mangler databehandleravtale med driftsleverandør. Datatilsynet fant ingen dokumenterte rutiner for å ivareta personopplysningslovens bestemmelser.

9.9 Velferd, forskning og helse

9.9.1 Tilsyn hos NAV

NAV-reformen berører hele befolkningen. I november i meldingsåret gjennomførte Datatilsynet tre kontroller med lokale NAV-kontorer. Tre pilotkontorer ble valgt. Disse var blant de første som slo sammen de tre tidligere funksjonene, arbeid, trygd og sosialtjenester. Kontorene har vært i drift i ca ett år.

En rekke funn ved de tre NAV-kontorene vekker bekymring.

Personkortet, som henter nøkkelinformasjon fra tre forskjellige fagapplikasjoner, har blitt fremhevet som et samhandlingsverktøy i NAV. Funnene under kontrollene viser imidlertid at Personkortet i praksis ikke blir oppfattet som tilstrekkelig. Mange av saksbehandlerne ved det lokale NAV-kontoret sitter nå med tilgang til alle tre fagsystemer fra de tidligere etatene, i tillegg til Personkortet. Anslagsvis har antallet brukere i fagapplikasjonene blitt doblet etter sammenslåingen. Datatilsynet kan heller ikke se at det har det har blitt etablert avhjelpende sikkerhetstiltak, som utvidet logging eller tilpasset tilgangsstyring.

Datatilsynet er bekymret for at fagapplikasjonen Arena (fra tidligere Aetat) er planlagt, og til en viss grad besluttet, benyttet som et oppfølgingsverktøy for NAV. Brukernes tilgang i Arena gis på et nasjonalt nivå.

Hovedfunnene ved tilsynene er:

1. Gjennom NAV-reformen har den enkelte medarbeider fått en betydelig større tilgang til personopplysninger. Dagens tildeling av tilganger er ikke egnet for å skape tillit, spesielt på grunn av manglende loggfunksjonalitet.
2. NAV synes å ha valgt et verktøy for å følge opp den enkelte tjenestemottaker uten at det etablert grunnleggende informasjonssikkerhetstiltak.
3. De kontrollerte kommunene har ved etableringen av NAV-kontorene ikke sørget for å følge opp sin selvstendige plikt til å sikre personopplysninger.
4. De kontrollerte kommunene hadde ikke tilfredstillende internkontroll.
5. Utformingen av publikumsmottakene ved NAV-kontorene gir store utfordringer i forhold til å sikre en fortrolig dialog.

9.9.2 Uredigerte journaler til NAV

I et lovendringsforslag åpner Arbeids- og inkluderingsdepartementet ytterligere for at NAV skal kunne samle inn uredigerte, fullstendige pasientjournaler.

Formålet med lovendringsforslaget er mer effektiv tilbakekreving av feilutbetalinger og bedre virkemidler for å bekjempe trygdemisbruk. NAV får nærmest ubegrenset tilgang til fullstendige og uredigerte pasientjournaler dersom forslaget skulle bli vedtatt. Om man

dømmer etter midlene NAV er foreslått å få, ser det ut til at oppklaring av trygdemisbruk oppfattes som viktigere enn oppklaring av drap. NAVs tilgang til journalene blir iallfall enklere enn politiets, selv når politiet etterforsker alvorlig kriminalitet. I tillegg får NAV utvidede hjemler til å samle inn informasjon fra andre enn helsevesenet. I realiteten får NAV en ”blancofullmakt” til å innhente alle opplysninger etaten selv mener er relevante, også om andre enn stønadsmottakeren.

9.9.3 Snikinnføring av forskningsdatabase over barnehagebarn

Innbakt i Kunnskapsdepartementets høringsforslag om ny barnehagelov ligger et forslag om innføring av en ny database over barnehagebarn. Tilsynet mener det er oppsiktsvekkende om det opprettes en slik database uten noen form for diskusjon

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

Det nye lovforslaget pålegger kommunene en plikt å rapportere til denne databasen. For at dette skal være mulig, foreslås det også at foreldre og foresatte pålegges en plikt til å oppgi barnets fødselsnummer til bruk i statistikk, analyse og forskning. Barnhager samler allerede inn barns fødselsnummer blant annet i barnehagesøknaden. Fødselsnummeret benyttes da for å skille barna fra hverandre. Denne bruken anses å oppfylle personopplysningsloven. Den nye bestemmelsen gir inntrykk av at barnehagene ikke har fødselsnummer fra før.

Datatilsynet har gjentatte ganger frarådet Kunnskapsdepartementet å innføre en ny nasjonal database uten en grundig utredning i forkant. Tilsynet mener det er viktig å kartlegge hva som er formålet med databasen, hvilke opplysninger den skal omfatte, hvem som skal forvalte den og hvilket tidsaspekt databasen vil ha. Fra høringsbrevet ser det ut til at Kunnskapsdepartementet ser for seg at de skal administrere registeret. Dette er ikke nødvendigvis mest hensiktsmessig. Andre aktører, som for eksempel Statistisk sentralbyrå, kan være bedre egnet til denne oppgaven.

Datatilsynet etterlyser også en klargjøring av når opplysninger eventuelt skal slettes fra databasen. Ettersom de aller fleste barn i løpet av sine første leveår er tilknyttet en barnehage, vil en slik database over tid inkludere nesten hele befolkningen. Når det i tillegg fremkommer at et forslag om å inkludere opplysninger om skolebarn er under utarbeiding, vil denne databasen på sikt kunne bli svært omfattende.

9.9.4 Ikke krav om nøkkelboks for å kunne motta hjemmetjenester

Kommuner kan ikke kreve at pleie- og omsorgstrengende personer har nøkkelboks utenpå huset, sier Sosial- og helsedirektoratet. Sosial- og helsedirektoratet vurderte ordningen med bruk av obligatoriske nøkkelbokser for brukere av pleie- og omsorgstjenesten, på spørsmål fra Hamar-politikeren Borgny Nygaard.

Nøkkelbokser er låsbare småskap der nøkkelen til inngangsdøren til den pleie- eller omsorgstrengende blir oppbevart. Boksen skal kunne åpnes med en universalnøkkel som pleierne bærer med seg.

Datatilsynet har erfart at flere personer oppfatter nøkkelboksene som stigmatiserende. Boksene vil blant annet kunne fungere som et synlig tegn på at det bor en hjelpetrengende person i huset. Tilsynet vurderte saken, og skrev at nøkkelboksene kan røpe et klientforhold, og at saken blir spesielt uheldig dersom nøkkelboks ved inngangsdøren blir et kriterium for å kunne få pleie og omsorg i eget hjem.

Sosial- og helsedirektoratet slutter seg til at det ikke kan stilles slike krav, og sier at dette prinsippet må være retningsgivende for alle kommuner i landet.

9.9.5 Tilsyn med rusomsorgen

Datatilsynet gjennomførte ti tilsyn innen rusomsorgen i meldingsåret. Tilsynsobjektene utgjorde et variert utsnitt av ulike frivillige organisasjoner, statlige og kommunale etater, forskningsinstitusjoner og helsetilbud som behandler personopplysninger om rusavhengige.

Innen rusfeltet registreres det personopplysninger av til dels svært sensitiv karakter, blant annet fysiske og psykiske helseopplysninger og opplysninger om straffbare forhold. Datatilsynet avdekket under tilsynene at omfanget av registrerte personopplysninger var betydelig.

Det var gjennomgående markante mangler ved programvaren som ble benyttet i rusomsorgen, blant annet i forhold til mangelfull og til dels fraværende logging, mangelfulle slettemuligheter og svært varierende tilgangsstyring, fra totalt fraværende til mer eller mindre tilfredsstillende.

I all hovedsak forelå det også mangler i forhold til internkontrollsystem og dokumenterte rutiner for behandling av personopplysninger. Informasjonen gitt til den registrerte var stort sett av muntlig karakter og mangelfull i forhold til personopplysningslovens krav. To virksomheter manglet konsesjon for sin behandling av sensitive personopplysninger.

Datatilsynet ser ikke behov for å gjennomføre flere tilsyn med rusomsorgen. Selv om tilsynene er gjennomført med tilsynsobjekter av relativt ulik karakter, er manglene etter personopplysningsloven relativt like. Funnene gir et godt grunnlag for videre arbeid innen området, noe som klart er nødvendig for å sikre grunnleggende rettigheter for de registrerte. Datatilsynet vil ta forholdene opp med blant annet hovedleverandøren av programvare til russektoren, samt direktorat og departement. Dette med tanke på å få bedret sikringen av personopplysingene til den enkelte, ikke bare som gruppe, men også som enkeltindivider. Datatilsynet kan ikke se at det er grunn til å behandle personopplysningene her annerledes enn det som er ønskelig i helsevesenet.

9.9.6 Ny helseforskningslov – unødvendig vanskelig for forskerne

I 2004 avga Nylennautvalget sin innstilling. Utredningen konkluderte med at rammeverket for medisinsk forskning var komplisert, fragmentert, utilgjengelig og til dels unødvendig byråkratisk. Sommeren 2007 ble Ot.prp. nr. 74 (2006-2007) Lov om medisinsk og helsefaglig forskning (helseforskningsloven), oversendt til Stortinget.

Datatilsynet er enig i vurderingen av at rammeverket er unødvendig komplisert og byråkratisk. Enklere søknadsprosedyrer og mindre byråkrati vil være positive tiltak, herunder forslaget om én postkasse for henvendelser. Det er også positivt at de forskningsetiske komiteer får en større og mer sentral rolle enn det som er tilfelle etter

dagens regelverk. Tilsynet er også tilhenger av innføring av et regelverk som er lettere tilgjengelig, slik at også personer uten juridisk spesialkompetanse kan sette seg inn i bestemmelsene.

Lovforslaget, slik Datatilsynet forstår det, har et betydelig forbedringspotensial på disse områdene. Tre ulike lover er riktignok samlet i én lov. Men denne er uklar, både i seg selv, og hva angår forholdet til omkringliggende regelverk. Dette medfører vanskeligheter både når man skal fastsette lovens anvendelsesområde, fastslå hvilke krav som stilles til sikring av opplysningene (informasjonssikkerhet), og avklare de involverte offentlige myndigheters ansvarsområder.

Bestemmelsen om lovens saklige virkeområde er ett av mange eksempler på at loven er uklar: Etter ordlyden skal loven ikke gjelde ved etablering av helseregistre. Helseforskning vil imidlertid nettopp innebære en etablering av helseregistre. Skal man legge vekt på ordlyden alene, vil opprettelse av alle slags helseregistre fremdeles måtte behandles av både Datatilsynet, Sosial- og helsedirektoratet og de etiske komiteene. Ordlyden undergraver altså alle muligheter for forenkling. Etter tilsynets vurdering bør ordlyden endres i samsvar med lovens intensjoner, om ikke annet av hensyn til forskerne.

Manglende informasjonssikkerhet

Personopplysningsloven inneholder klare krav til informasjonssikkerhet, men det er lite som tyder på at disse kravene skal gjelde også for helseforskning. Etter Datatilsynets syn kan ikke forskere fristilles på dette området. De samme krav til informasjonssikkerhet bør gjelde for medisinsk forskning som på andre områder hvor det behandles helseopplysninger. Det er da nødvendig at helseforskningsloven enten kompletteres med egne sikkerhetsbestemmelser, eller at det inntas en tydelig henvisning til personopplysningslovens krav til informasjonssikkerhet.

Også Datatilsynets egen myndighet etter lovforslaget er uklar. Det legges opp til at de forskningsetiske komiteene skal forhåndsgodkjenne prosjekter som medfører forskning på helseopplysninger. Datatilsynet og Helsetilsynet er tillagt delt tilsynsmyndighet, og skal gjennomføre etterkontroller av forskningsprosjektene. For Datatilsynet er det imidlertid uklart om rollen blir å påse at prosjektene gjennomføres i henhold til de forskningsetiske komiteers vedtak, eller om vi skal påse at de gjennomføres i samsvar med tilsynets forståelse av loven.

Både de etiske komiteene og Datatilsynet er, i medhold av lov, tillagt en særlig uavhengig stilling. For forskningsmiljøet er det viktig å kunne ha tillit til at en forhåndsgodkjenning ikke senere settes til side av Datatilsynet. En ordning der Datatilsynet skal føre tilsyn i henhold til de etiske komiteers forståelse av regelverket, vil på sin side komme i konflikt med tilsynets rolle som en selvstendig og uavhengig tilsynsmyndighet.

Uthuling av prinsippet om samtykke

Forslagets formelle hovedregel er at forskning på helseopplysninger skal være basert på samtykke fra den som opplysningene gjelder. Dette er i tråd med både forskningsetiske og personvernmessige grunnprinsipper, nasjonalt og internasjonalt.

Lovforslaget inneholder imidlertid så mange muligheter til å sette samtykket til side, at den reelle og praktiske hovedregelen lett vil bli at samtykke blir unødvendig.

Lovforslaget innfører også et nytt rettslig begrep, nemlig ”bredt samtykke”. Denne formen for samtykke strekker seg lengre enn det som aksepteres i dag, og kan sammenlignes med

at man inngår en avtale uten å få lov til å lese avtalevilkårene. At det, etter utkastet til helseforskningsloven, defineres som et "samtykke", er etter tilsynets vurdering uheldig. Man står i fare for å uthule den enkeltes grunnleggende rett til informasjon og selvbestemmelse. Dette kan utvikle seg til en belastning for det nødvendige tillitsforholdet mellom samfunnet og legen.

Selv om tanken om én lov kan være besnærende, viser forslaget at det er vanskelig i praksis å forene regelverkene. Når forslaget i tillegg innebærer en økt trussel mot personvernet, ba Datatilsynet Stortinget om at de positive og negative virkningene ved loven skulle vurderes nærmere.

9.9.7 Tilsyn: Tilgang til helseopplysninger

Høsten 2007 ble det gjennomført en større kontroll med fokus på tilgang til helseopplysninger ved Sykehuset i Vestfold HF.

Datatilsynet registrerer på bakgrunn av kontrollen med Sykehuset i Vestfold at det fremdeles er helseforetak som behandler helseopplysninger i journalsystemer som er direkte uegnet til å ivareta fortroligheten ovenfor pasienten i et moderne sykehusmiljø. Det ble avdekket at svært vide tilganger var gitt på grunn av systemets beskaffenhet. De vide tilgangene var supplert med til dels fraværende loggfunksjonalitet. Det kom under kontrollen frem en hendelse hvor et høyt antall ansatte hadde gjort uautorisert oppslag i en del av informasjonssystemet som hadde etablert logging. Hendelsen var etter Datatilsynets syn ikke adekvat fulgt opp fra foretakets side.

Dokumentkontrollene er per skrivende stund ikke ferdigbehandlet. Det er her også parallelle saker hos Helsetilsynet i forhold til det involverte helsepersonellets opptreden. Datatilsynet registrerer flere saker av denne karakteren. Datatilsynet legger til grunn at dette skyldes at et økt fokus på informasjonssikkerhet i sektoren medfører at flere av foretakene evner å avdekke noe av snikingen i journaler.

9.9.8 Tilsyn: Urettmessig innsyn i pasientjournaler

Datatilsynet ble sommeren 2007 kontaktet av Legeforeningen i forbindelse med et innsyn i pasientjournal ved Ullevål universitetssykehus HF. Saken gjaldt en person som var ansatt ved sykehuset, og som også hadde vært pasient samme sted. Vedkommende oppdaget at fire personer uten behandlerrelasjon hadde gjort oppslag i hans journalnotater. Den ansatte oppdaget forholdet ved gjennomgang av journalloggen.

Tilsynet rettet en henvendelse til sykehuset, og ba om flere opplysninger. Dette omfattet blant annet bakgrunnen og formålet med hvert enkelt oppslag som ikke var knyttet direkte til behandlingssituasjonen. Det ble også bedt opplyst om personene som foresto oppslagene handlet på vegne av andre eller i medhold av instruks. Tre av personene hadde kun foretatt feiloppslag i kontaktoversikten, og ikke lest selve journalen.

Snoking

Én av personene, et tidligere ansatt helsepersonell ved sykehuset, foretok hele 37 oppslag i journalsystemene over en periode på en måned i 2004. Oppslagene er i hovedsak foretatt i selve journalen. Vedkommende har ikke hatt noen behandlingsmessig eller annen grunn for innsyn i klagers pasientjournal. Såkalt "aktualiseringsrett" skal være benyttet, og det er

anført at formålet med oppslagene har vært ”fagoppfølging”. Oppslagene fremstår som omfattende og kan gi inntrykk av å være systematisk gjennomført.

Helsepersonellet har i mail-korrespondanse med sykehuset innvendinger til påstanden om ulovlig tilgang. Vedkommende uttaler at: ”det forhold som beskrives er meg fullstendig ukjent og uforståelig”. Det antydes videre at det må ha skjedd en feil, eller at noen andre har brukt vedkommendes tilgang uten at han/hun har visst om det. Sykehuset har opplyst til Datatilsynet at det ikke har vært mulig å fastslå hva som er korrekt faktum, og at saken er meldt som avvik til Helsetilsynet i Oslo og Akershus for videre oppfølging. Ettersom vedkommende ikke lenger arbeider ved sykehuset, er arbeidsrettslige reaksjoner ikke lenger aktuelt.

Datatilsynet ser svært alvorlig på denne type situasjoner. Redegjørelsen fra helsepersonellet fremstår som lite sannsynlig. I beste fall gir redegjørelsen inntrykk av svært kritikkverdig omgang med personlige adgangskoder til journalsystemene.

Når det gjelder helseforetaket, kan det synes som om tilgangskontrollen ikke er tilfredsstillende innrettet. Helsepersonell bør ikke ha en systemtilgang som lar dem gjøre slike oppslag om pasienter de ikke har et behandlerforhold til.

9.9.9 Snoking i pasientjournaler - behov for lovendring

Helse- og omsorgsdepartementet sendte i meldingsåret ut et forslag om å tydeliggjøre at det er forbudt å tilegne seg pasientopplysninger urettmessig. Datatilsynet er tilfreds med forslaget, men foreslår at man vurderer å ta inn et supplement. Tilsynets forslag er at det i tillegg tilrettelegges for at alle pasienter kostnadsfritt får anledning til å se sine egne journallogger. Pasienten vil på denne måten få anledning til selv å gjennomgå hvem som har lest i journalen. Journalloggen kan enten sendes til pasienten med jevne mellomrom, eller utleveres sammen med journalutskrift/epikrise etter utskriving.

Formålet med rettigheten er å gi pasienten bedre kontroll over hvem som åpner journalen av ren nysgjerrighet. Ved at pasientene får tilgang til loggene, kan de selv oppdage hvor ofte – og hvem – som har lest i journalene deres.

Personvernrisikoen i helsesektoren har økt som følge av overgangen fra papir til elektroniske pasientjournaler (EPJ). Problematikken er særlig knyttet til at mer informasjon er lettere tilgjengelig for flere, lettere å spre til uvedkommende, og i den grad opplysningene først er spredd, er det vanskeligere å begrense skaden for pasientene som er rammet.

En fordel med elektroniske løsninger er imidlertid muligheten til å loggføre alle oppslag, altså en automatisk registrering av hvem som har åpnet hvilke journaler og hvor lenge de har vært åpne. Slike logger eksisterer i dag, men tilsynets erfaring tilsier at disse ikke blir kontrollert eller fulgt opp på en tilfredsstillende måte.

Det er vanskelig å angi et kvalifisert omfang av uautoriserte oppslag i pasientjournaler. Mulighetene for misbruk er definitivt til stede, og flere misbrukssaker er forelagt tilsynet.

En MMI-undersøkelse, gjort på oppdrag fra KFO og gjengitt i Dagbladet 5. juni 2005, anfører at 86 prosent av de ansatte i helsevesenet bekrefter at det er utbredt å se i journalene ut over det som er nødvendig. Undersøkelsen gir i beste fall uttrykk for at en stor andel

ansatte i helsevesenet ikke er trygge på at journalopplysninger blir håndtert på en god nok måte.

Datatilsynet har lang erfaring med tilsyn rettet mot helseforetak. Tilsynene har vist at det oppstår store misbruksmuligheter når man kombinerer vid tildeling av tilgangsrettigheter til journalsystemene, mangelfulle systemfunksjoner som kan begrense tilgangen, og lav reell kontroll med berettigelsen av oppslag i systemet.

Det har vist seg å være vanskelig å avdekke uautoriserte oppslag. Søkelyset rettes gjerne mot uautorisert tilgang til opplysninger om kjendiser og ansatte, men tilsynet har grunn til å tro at problemet er mer omfattende i forhold til opplysninger om egen bekjentskapskrets. Dette kan være langt vanskelig å avsløre - rett og slett fordi foretaket ikke kjenner til hvem som er familiemedlemmer, venner eller bekjente av den enkelte. Pasientene derimot, kan se om den som har lest journalen er noen de kjenner eller vet hvem er.

For Datatilsynet er det viktig at både pasienter og ansatte ved norske helseforetak føler seg trygge på at journalopplysninger behandles med behørig respekt for pasientenes integritet.

9.9.10 Datainnsamling bygd på medisinsk uforsvarlig prøvetaking – Aker sykehus - Hoftebruddsprosjektet

For fem år siden ble det ved Aker universitetssykehus HF igangsatt en prospektiv undersøkelse knyttet til risikofaktorer for hoftebrudd hos eldre over 65 år. Prosjektets kirurgiske del innebar innhenting av muskel-og benbiopsi i forbindelse med den operative behandlingen. Datatilsynet ga konsesjon til dette i 2003. Datatilsynet varslet om at konsesjonen bortfalt i løpet av meldingsåret. Årsaken til dette er den manglende overholdelsen av regelverket.

Vevsprøvene og alle personopplysninger knyttet til, eller utledet fra disse, ble pålagt slettet og destruert på forsvarlig vis.

Uforsvarlig prøvetaking

I 2005 påla Statens helsetilsyn Aker universitetssykehus HF å stanse innhentingen av biopsier. Årsaken til pålegget var blant annet at biopsi-takingen førte med seg en tilleggsrisiko for pasientene, uten at risikoen kunne forsvares som en del av den medisinsk-faglige behandlingen.

Helsetilsynet fattet vedtak om å gi advarsel til to av prosjektdeltakerne. Vedtaket ble opprettholdt av Statens helsepersonellnemnd. Også Arbeids- og inkluderingsdepartementet og Sosial- og helsedirektoratet uttalte seg kritisk til prosjektet. Både Helsetilsynet og Helsepersonellnemnda har lagt til grunn at prøvetakningen, uavhengig av samtykkekompetanse, var uforsvarlig. Sett hen til den massive kritikken, fremstår det som Datatilsynet er villedet i søknadsprosessen.

Pålegget om å stanse innhentingen av biopsier ble fulgt, etter det Datatilsynet er informert om. Inklusjon og klinisk oppfølgning av prosjektpasientene ble imidlertid videreført. Etter det Datatilsynet forstår, var ikke de øvrige delene av prosjektet omfattet av Helsetilsynets kritikk.

Regional Etisk Komité (REK) har avgitt uttalelse om at det ikke er etisk forsvarlig å bruke opplysninger utledet av biologisk materiale som er innsamlet i strid med kravet til forsvarlig helsehjelp.

På denne bakgrunnen fant Datatilsynet det nødvendig å fatte vedtak om sletting av alle personopplysninger knyttet til, eller utledet fra, disse prøvene.

For Datatilsynets vurderinger av konsesjoner til forskningsprosjekter, er det en forutsetning at prosjektet er i samsvar med annen lovgivning. Dersom Datatilsynet hadde vært kjent med alle sider av hvordan prosjektet utviklet seg, ville konsesjon ikke blitt innvilget.

Kritikkverdig informasjon

Datatilsynet påpeker også at håndtering av informasjonen til de inkluderte og benyttelsen av samtykkeskriv i denne saken fremstår som svært kritikkverdig. Dersom konsesjonsinstituttet skal fungere etter sin hensikt, er Datatilsynet avhengig av at forskningsprosjekter gjennomføres i tråd med oversendt prosjektbeskrivelse. En konsesjon er en tillatelse, som i stor grad forutsetter tillit til at informasjonen gitt av forskeren er korrekt.

9.10 Handel, finans og forsikring

9.10.1 Sletting i nettbutikker og hoteller

På ti tilsyn med hovedformål å se på sletting av kundeopplysninger ved hoteller og nettbutikker, fant Datatilsynet lagring av opplysninger som skulle vært slettet. Det ble avdekket at det langt på vei skyldtes et uklart forhold til regnskapslovgivningen.

Regnskapslovgivningen pålegger lagring av visse typer opplysninger i en gitt periode. De kontrollerte virksomhetene hadde IT-systemer med tett integrasjon mellom regnskapsopplysninger og kundeopplysninger. Dette gjør det vanskelig å skille mellom opplysninger som skal oppbevares og opplysninger som skal slettes.

9.10.2 Tilsyn hos eiendomsmeglere

Det ble høsten 2007 gjennomført fem tilsyn med ulike eiendomsmeglerforetak, hvorav én virksomhet drev med utleie av bolig. Datatilsynet fant en overraskende manglende kjennskap til personopplysningsloven.

Eiendomsmeglerbransjen behandler som hovedregel ikke sensitive personopplysninger, men det behandles opplysninger om økonomiske forhold. Slike opplysninger oppfattes av publikum som svært følsomme, og informasjonsmengden bransjen behandler må i tillegg antas å være relativt stor.

Den manglende kjennskapen som ble avdekket under tilsyn, synes å være gjennomgående for hele bransjen. Datatilsynet vil ta forholdene opp med bransjen for å sikre bedre kunnskaper om personopplysningsloven.