Datatilsynet

Justis- og politidepartementet
Postboks 8005 Dep

0030 OSLO

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
200904400 ES HAJ	09/00944-2 /HTL	30. oktober 2009

Høringsuttalelse - etterkontroll av personopplysningsloven

Postadresse: Postboks 8177 Dep 0034 OSLO | Kontoradresse: Tollbugt 3 | Telefon: 22 39 69 00 | Telefaks: 22 42 23 50 | Org.nr: 974 761 467 | Hjemmeside: www.datatilsynet.no

1. Innledning

Datatilsynet viser til høringsbrev av 3. juli 2009 vedrørende etterkontroll av personopplysningsloven.

Siden tilblivelsen av personopplysningsloven har både samfunnsmessige endringer og den teknologisk utvikling skapt et behov for å se på regelverket med nye øyne. Datatilsynets erfaringer viser at enkelte bestemmelser ikke har fungert som forutsatt eller at bestemmelser kunne ha vært formulert mer hensiktsmessig.

I høringsnotatet bes det om høringsinstansenes syn på de vurderinger og forslag som fremkommer av vedleggene til høringsbrevet. Datatilsynet har videre benyttet anledningen til å kommentere enkelte sider ved loven som ikke er direkte behandlet i høringsnotatet eller vedleggene. Datatilsynet viser i den sammenheng til NOU 1997: 19 *Et bedre personvern* og Ot.prp. nr. 92 (1998-99) *Om lov om behandling av personopplysninger (personopplysningsloven).*

Det påpekes at en av intensjonene med loven var at enkeltindividet skulle få større råderett over egne personopplysninger. Dette ble fulgt opp med rettigheter til enkeltindividet, herunder rett til innsyn og retting av feilaktig informasjon, samtidig som den behandlingsansvarlige måtte forholde seg til en rekke plikter, blant annet sletting av opplysninger og plikten til å gi informasjon. Datatilsynet fikk, sammen med daværende Moderniseringsdepartementet, gjennomført to undersøkelser om enkeltpersoners og virksomheters kunnskaper og holdninger til personvern. Undersøkelsene, som ble gjennomført av Transportøkonomisk institutt i 2005, viste at det gjennomgående var lite kunnskap om de rettigheter og plikter som oppstilles i loven både hos privatpersoner og virksomheter. Dette er omtalt i utredningen fra Schartum og Bygrave uten at det etter Datatilsynets vurdering har fått tilstrekkelig oppmerksomhet i lovarbeidet generelt.

Personvernkommisjonens rapport 2009: 1 *Individ og integritet* tar opp en rekke personvernspørsmål av til dels overordnet karakter. Datatilsynet har gitt sine merknader til denne i brev til FAD av 28. august 2009, jf. vedlegg nr. 1. Enkelte av temaene som behandles her er sentrale i vurderingen av hvordan personvernregelverket bør se ut fremover. Vi viser blant annet til gjennomgangen av personopplysningslovens § 7 og spørsmålet om lovregulering av barn og unges personvern. Datatilsynet legger til grunn at de relevante delene av høringssvarene blir tatt i betraktning i forbindelse med lovrevisjonen. Tilsynet har forstått det slik at årsaken til at kun deler av personvernlovgivningen ble satt ut til Schartum og Bygrave var at Justisdepartementet (JD), FAD og Datatilsynet skulle se på øvrige sider ved loven. En av konsekvensene ved denne delingen er at det er til dels vanskelig å få oversikt over hva som er det samlede forslaget fra departementet. Det fragmenterte underlagsmaterialet for høringen har også gjort arbeidet med høringsuttalelsen mer komplisert enn nødvendig, og Datatilsynet antar ut fra dette at instanser med grunnleggende kjennskap til personvernregelverket har hatt en stor fordel i dette arbeidet, mens andre organer og virksomheter kan ha hatt uforholdsmessige utfordringer.

For Datatilsynet er det viktig å understreke at det kun bør gjøres endringer i regelverket dersom man ønsker å endre gjeldende rett, eller at dagens bestemmelser ikke gjenspeiler hva som er gjeldende rett. Dersom det ikke er tilfelle, og ordlyden verken byr på uforholdsmessige utfordringer i praksis eller bør endres av pedagogiske grunner, bør bestemmelsene få stå uendret. Det bemerkes at ikke alle de foreslåtte endringene synes å være begrunnet ut fra noen av disse hensynene, men kan bære preg av å være en ren teoretisk øvelse. En endring av en bestemmelse vil lett bli oppfattet som et utrykk for en endring av rettstilstanden. Likeledes vil innføring av nye begreper skape ny tolkningstvil og bør også unngås hvis man ikke har til hensikt å gi et nytt materielt innhold.

Datatilsynets høringsuttalelse vil i all hovedsak følge den samme kronologien og tematiske inndeling som departementets høringsnotat.

1.1. Innledende kommentarer til høringen

Personvern er ikke bare noe institusjoner og virksomheter skal forholde seg til. Personvern forholder seg like mye til ordet "person" som vern. Som det fremkommer av den gjeldende angivelse av lovens formål er dette personrelatert, og kan ikke bare sees på som et "vern" hvor forpliktelsen ligger på den eller de institusjoner eller virksomheter som har opplysninger om mange enkeltindivider. Som tilsynsmyndighet og regelverksforvalter ser Datatilsynet viktigheten av at personvernet også må eksistere mellom enkeltindivider, og materialisere seg i måten vi oppfatter og forstår begrepet personvern. Datatilsynet har derfor foreslått en tilføyelse i lovens § 1 nettopp for å presisere at det er den enkeltes ansvar å håndtere opplysninger om andre innenfor grensene for det vi kan kalle alminnelig folkeskikk og gjensidig respekt for andre.

I lovrevisjonsarbeidet er det videre viktig for Datatilsynet å kommunisere at på enkelte punkter ønsker vi en endring i forhold til dagens praksis. Vurderinger etter personopplysningslovens § 7 er omtalt i utredningen, og som det vil fremkomme nedenfor, ønsker tilsynet å ta tak i denne problematikken.

Tilsynets erfaringer, og de spørsmål Datatilsynet erfaringsmessig blir stilt overfor vedrørende kredittopplysningsvirksomhet, trekker i retning av at slik virksomhet bør reguleres i et særskilt regelverk. Det vil blant annet føre til enklere prosesser i fremtiden dersom utviklingen på dette området skulle foranledige et behov for endringer av regelverket.

Bruk av, og et ønske om bruk av, fødselsnummer i ulike sammenhenger, er også en gjenganger blant de vurderinger som tilsynet stilles overfor i det dagelige. Mange aktører, både private og offentlige, ønsker å benytte denne identifikatoren, og vi erfarer at mange bruker store ressurser på å argumentere mot Datatilsynet i spørsmål angående behandling av fødselsnummer. Som det vil fremkomme har vi sett på denne problemstillingen i vårt høringssvar. Fødselsnummeret benyttes i mange sammenhenger som den unike nøkkel for identitetsfastsettelse. Slik bruk medfører et misbrukspotensiale. Vi ser også at det utenfor personopplysningslovens anvendelsesområde vil være utfordringer som har nære forbindelser med personvern. Et eksempel er utlevering av personopplysninger etter offentlighetsloven, hvor publikum kan kreve innsyn i dokumenter som inneholder fødselsnummer.

Fødselsnummeret er i seg selv ikke en sensitiv personopplysning, men bør like fullt beskyttes mot offentliggjøring. Denne problematikken og andre tilstøtende utfordringer for fremtiden er også omtalt i det følgende høringssvaret.

Behandling av spørsmål rundt bruk av biometriske kjennetegn har, etter vår oppfatning, mange likhetstrekk med vurderinger knyttet til bruk av fødselsnummer, og er et område tilsynet ønsker å ha god kontroll over. Det bør ikke åpnes for at slike metoder for identifisering benyttes der det ikke er nødvendig og følger av en reell vurdering av om det foreligger et tungtveiende behov.

Erfaringer fra de stedlige kontrollene Datatilsynet har foretatt har avdekket at det er mange virksomheter som har vanskeligheter med å se sammenhengen mellom bestemmelsene om internkontroll og informasjonssikkerhet og at det igjen medfører at innholdet i bestemmelsene blir uklart. Vi foreslår at rekkefølgen på bestemmelsene får en mer naturlig orden. Informasjonssikkerhet er et element i internkontrollen, og derfor bør regelen som pålegger internkontroll stå foran de øvrige pliktbestemmelsene.

Mer generelt ønsker Datatilsynet å beholde konsesjonsinstituttet fordi vi har erfart at det fortsatt er behov for en viss forhåndskontroll, samt at konsesjonsplikten kan være en hensiktsmessig måte å regulere ulike bransjer, men vi foreslår at tilsynet gis mulighet til å dispensere fra en ellers obligatorisk konsesjonsplikt.

I det videre har tilsynet forsøkt å systematisere kommentarene knyttet opp til bestemmelser i dagens lovtekst og høringsbrevets tematikk.

2. Formålsbestemmelsen

Etter sin ordlyd omfatter dagens formålsbestemmelse alle som behandler personopplysninger. Tilsynets erfaring er imidlertid at publikum forventer at Datatilsynet skal våke over deres personvern. Tilsynet sitter igjen med et inntrykk av at enkeltpersoner, både i egenskap av å være behandlingsansvarlig og som registrert, har forventninger om at det er tilsynsorganet som i praksis skal ivareta borgernes personvern. Særlig gjelder dette forholdet mellom enkeltpersoner. For å presisere at loven retter seg mot alle og enhver foreslår vi en endring i personopplysningslovens § 1, 2. ledd.

Forslaget presiserer at det er hver og én av oss sitt eget ansvar å følge lovens intensjon og regelsett ved behandling av personopplysninger. Datatilsynet er klar over at loven gjelder "enhver" i dag også, men erfaring viser at dette er noe Datatilsynet ofte må forklare publikum. Den raske teknologiske utvikling muliggjør innsamling, systematisering og publisering av store mengder opplysninger også for enkeltpersoner, og tilsynet mener det er viktig at lovens formålsbestemmelse har en form som tydeliggjør at ved slik behandling av opplysninger om andre personer følger også et rettslig ansvar.

Datatilsynet foreslår derfor at 2. ledd i § 1 får følgende innhold:

Loven skal bidra til at enhvers behandling av personopplysninger skjer i samsvar med grunnleggende personvernhensyn og med respekt for personlig integritet, privatlivets fred, og opplysningenes kvalitet.

3. Definisjonene i personopplysningslovens § 2

3.1. Personopplysning

3.1.1. Personopplysningenes form

Datatilsynet vil innledningsvis bemerke at i praksis er det sjeldent at personopplysningers form eller uttrykksmåte skaper tvil om hvorvidt loven vil komme til anvendelse eller ikke. Å foreta endringer av loven på dette punkt fremstår derfor som unødvendig. Datatilsynet er i tillegg av den oppfatning at hensynet til et teknologinøytralt regelverk best ivaretas dersom man *ikke* lister opp ulike former eller uttrykksmåter, slik utrederne foreslår. Tilføyelsen kan få preg av en presisering som innskrenker lovens virkeområde, og vil trolig gi rom for nye tolkningsproblemer. Datatilsynet vil derfor ikke anbefale at lovteksten endres på dette punktet.

3.1.2. Enkeltperson

Datatilsynet vil presisere at det ikke har vært tvil i praksis om at loven bare gjelder enkeltpersoner, dvs avgrenset mot juridiske personer og døde. Tilsynet stiller derfor spørsmål ved behovet for den foreslåtte endringen, utover eventuelle pedagogiske gevinster. På den annen side vil tilføyelsen neppe medføre at det skapes ny tokningstvil. Datatilsynet anbefaler derfor at ordlyden endres i tråd med forslaget.

Datatilsynet har tidligere[1] argumentert for at loven bør gjelde for opplysninger om døde personer, også i de tilfeller hvor opplysningene om den døde ikke samtidig sier noe om levende personer. Tilsynet vil hevde at den personlig integritet bør gis vern i noen tid etter personens død, for å ivareta hensynet til den registrertes *ettermæle*. Hvordan borgernes opplysninger behandles etter ens død, har naturlig nok betydning for hvilken trygghet den enkelte opplever mens man fortsatt er i live.

Artikkel 29-gruppen understreker at selv om direktivet ikke gir direkte vern for døde personer, så står medlemsstatene fritt til å gi døde personer vern i henhold til nasjonal lovgivning[2].

[1] Høringsuttalelse til personopplysningsloven
[2] Op 4/2007 on the consept of personal data

3.1.3. Opplysninger og vurderinger

Datatilsynet vil presisere at det heller ikke på dette området har vært tvil av betydning om hvordan loven er å forstå. Tilsynet er av den oppfatning at gjeldende ordlyd rent språklig favner noe videre enn forslagets ordlyd. Begrepet "informasjon" kan forstås dit hen at det stilles et krav om at opplysningene skal være av en viss kvalitet. Mens ukvalifisert synsing utvilsomt faller inn under begrepet "vurderinger", vil det være mindre naturlig å kalle slik synsing for "informasjon". Tilsynet frykter at den foreslåtte ordlyden vil kunne innskrenke lovens virkeområde, og at den i det minste åpner for tvil om virkeområdet. Datatilsynet anbefaler derfor ikke at lovens ordlyd endres på dette punktet.

3.1.4. Humant biologisk materiale

Datatilsynet støtter ikke forslaget om å uttrykkelig unnta humant biologisk materiale fra personopplysningsbegrepet. Dette skyldes at man pr i dag ikke fullt ut overskuer hvilke muligheter som ligger i behandling av slikt materiale i fremtiden. Utviklingen peker i retning av at biologisk materiale i økende grad vil kunne gi utfyllende opplysninger om enkeltpersoners spesifikke egenskaper. Det biologiske materiale vil i så måte representere en kilde til slik kunnskap, i likhet med for eksempel elektroniske spor, og som kan danne grunnlag for slutninger om spesifiserte mønstre om adferd. Verken elektroniske spor eller biologisk materiale vil i alle sammenhenger være personopplysninger, men blir det i det øyeblikk slikt materiale med iboende informasjon knyttes til et enkeltindivid. Datatilsynet er bekymret for at en klar avgrensning i lovverket vil avskjære tilsynet fra kvalifiserte vurderinger i slike grensetilfeller.

Høyesterett har uttalt følgende om humant biologisk materiale[3]:

"Humant biologisk materiale står i en meget spesiell stilling ved at analyser nå, og spesielt i lys av framtidig kunnskap med hittil ukjente metoder, kan gi tilgang til opplysninger om personer, jf. NOU 2005:1 side 185 annen spalte. Slikt materiale er vesensforskjellig fra helseopplysninger inntatt i dokument eller annet ved at nye opplysninger kan " hentes ut" av humant biologisk materiale, jf. NOU 2001:19 om biobanker side 99 første spalte. Behovet for personvern for levende og døde er således spesielt sterkt ved at biologisk materiale kan gi tilgang til bestemte personers gener, sykdommer, lyter og andre egenskaper."

Datatilsynet vil derfor ikke anbefale at det vedtas en bestemmelse som kategorisk utelukker at loven får anvendelse. Behandlingskravet i personopplysningslovens § 3, og omfattende særregulering[4], medfører uansett at loven sjelden kommer til anvendelse ved behandling av slikt materiale.

---

[3] Rt 2006.90

[4] For eksempel biobankloven, bioteknologiloven og helseregisterloven

3.1.5. Kravet om identifikasjon

Datatilsynet støtter departementets vurderinger og anbefaler at lovteksten endres i tråd med forslaget.

3.1.6. Pseudonymisering

Datatilsynet anbefaler ikke at behandling av pseudonyme opplysninger unntas fra lovens virkeområde. Dette gjelder selv om pseudonymiseringen er gjort i samsvar med nærmere gitte retningslinjer. Tilsynet anser at en fleksibel ordning, hvor lovens krav i det konkrete tilfellet tolkes i lys av at opplysningene er pseudonyme, bør videreføres. Den viktigste begrunnelsen for tilsynets oppfatning er at det hersker stor reell usikkerhet omkring begrepene avidentifiserte, pseudonymiserte og anonyme data. I mange tilfeller er det behov for å veilede virksomhetene for at pseudonymiseringen skal kunne bli reell. Muligheten for identifisering vil alltid være tilstede i ulik grad, hvilket gjør at effekten av tiltaket kan forringes. At opplysninger er psedonymisert vil likevel innebære vesentlige lettelser for de behandlingsansvarlige, for eksempel tillegges det stor vekt ved tilsynets håndheving av de plikter som følger av dagens §§ 13 og 14.

Datatilsynet støter ofte på tvil og misforståelser knyttet til vurderingen av hvorvidt en opplysning er identifiserbar eller ikke, særlig hvorvidt opplysninger som er pseudonyme i praksis er å anse som anonyme, og derfor faller utenfor lovens virkeområde. Det er også mye usikkerhet rundt når opplysninger er å anse som henholdsvis avidentifiserte eller pseudonyme. I helseregisterlovens § 2 nr 2, 3 og 4, defineres de ulike variantene av helseopplysninger, basert på graden av identitet: avidentifiserte opplysninger, pseudonyme opplysninger og anonyme opplysninger. Tilsynet ber departementet vurdere å innta en definisjon av avidentifiserte og pseudonyme opplysninger i personopplysningsloven.

3.1.7. Sensitive opplysninger

Datatilsynet støtter departementets vurderinger, og anbefaler at lovteksten endres i tråd med forslaget.

3.2. Behandling av personopplysninger

Departementet bemerker at det i praksis kan være vanskelig å oppstille et klart skille mellom én og flere behandlinger. Datatilsynet kan ikke se at dette er en problemstilling som har praktisk betydning. Tilsynet definerer i sin praksis en behandling ut fra formålet. Dersom det er aktuelt med flere ledd eller operasjoner i prosessen med å nå et bestemt formål, så vil dette ses som én behandling. Innen forskning vil for eksempel ett definert forskningsprosjekt representere ett formål, og være å anse som én behandling. Likeledes vil personaladministrasjon være å anse som ett behandlingsformål, selv om det innebærer innhenting, sammenstilling, lagring og utlevering av opplysninger. På den annen side stiller tilsynet krav om at behandlingsformålet må være konkret angitt, jf personopplysningslovens § 11. Det finnes derfor grenser for hvor overordnet eller generelt formålet kan defineres.

Tilsynet har erfart at behandlingsbegrepet ikke er lett tilgjengelig for behandlingsansvarlige og andre lovanvendere, og ønsker derfor en lovendring som tydeliggjør sammenhengen mellom behandling og formål. Dette kunne for eksempel ha skjedd gjennom en tilføyelse i definisjonen:

"...som foretas for å nå et uttrykkelig angitt formål".

3.3. Personregister

Det vises til høringsuttalelsens pkt. 3.1 om personopplysningslovens § 3.

3.4. Behandlingsansvarlig

Datatilsynet støtter at lovens ordlyd åpner for at ulike rettssubjekter kan ha felles og delt behandlingsansvar for en behandling. Dette under forutsetning av at de ansvarlige ikke står i et over- og underordningsforhold til hverandre. Felles eller delt ansvar antas å være særlig praktisk i forbindelse med behandling som skjer innenfor konserner.

Datatilsynet anbefaler imidlertid at forslaget til ordlyd justeres noe. I forslaget er ansvaret lagt til den som innehar kompetansen til å bestemme, jf uttrykket "kan bestemme". I gjeldende definisjon er ansvaret tillagt den som faktisk bestemmer. Tilsynet er usikker på om denne endringen er tilsiktet, og savner i så fall en begrunnelse for det.

4. Personopplysningslovens saklige virkeområde

4.1. Personopplysningslovens § 3 første ledd bokstav a

I høringsnotatet punkt 2.1.2 omtales Personvernnemndas sak PVN-2005-01. Etter nemndas syn skal man i vurderingen av om noe er et elektronisk hjelpemiddel etter personopplysningsloven § 3 første ledd bokstav b legge "avgjørende vekt på om behandlingen skjer automatisk , uten intervensjon av mennesker." På denne bakgrunn ble et lydopptak, som ble startet og stanset manuelt, ikke ansett å være behandling med "elektroniske hjelpemidler".

Etter Datatilsynets vurdering innebærer nemndas forståelse av begrepet en innskrenkende tolkning av ordlyden i personopplysingslovens § 3 første ledd bokstav a, som det er vanskelig å finne støtte for i forarbeidene[5] eller personverndirektivet. Personvernhensyn taler også klart imot nemndas forståelse av begrepet "elektronisk hjelpemidler".

For å avklare tolkningstvil på dette punktet tiltrer Datatilsynet departementets forslag om å endre ordlyden i personopplysningsloven § 3 første ledd bokstav a, slik at det går klarere frem at ikke bare fullstendig automatiske prosesser er omfattet av loven.

[5] Se for eksempel Ot.prp.nr.92 (1998-1999) i merknadene til bestemmelsen på side 104 til 105 og pkt 4.1.

4.2. Personopplysningsloven § 3 annet ledd

Datatilsynet kan ikke se at det er behov for å endre ordlyden i personopplysningsloven § 3 annet ledd som følge av den såkalte Lindqvist-saken[6]. Det er fullt mulig å tolke bestemmelsen slik at kravet om at et formål er privat eller personlig, innebærer at behandlingen skjer innenfor en lukket sfære. Uansett vil et fokus på *formålet* med behandlingen normalt gi samme tolkningsresultat som når det legges vekt på behandlingens *karakter*. Datatilsynet er heller ikke kjent med det i praksis har vært problematisk å fortolke ordlyden i samsvar med EF-domstolens avgjørelse.

Datatilsynet er også av den oppfatning at den foreslåtte endringen ikke nødvendigvis vil gjøre innholdet i lovteksten klarere. Det kan være enklere å fastslå kjernen i unntaket ved å ta utgangspunkt i formålet med behandlingen og ikke behandlingskonteksten. Formålet med behandlingen står også sentralt ved tolkningen av mange andre bestemmelser i loven.

På bakgrunn av det ovennevnte støtter Datatilsynet ikke departementets forslag om å justere ordlyden i personopplysningsloven § 3 annet ledd.

Datatilsynet er imidlertid enig med departementet i at både praktiske og pedagogiske hensyn tilsier at man bør ha en supplerende regel som sier noe om i hvilken grad publiseringer på Internett kan skje uten at loven kommer til anvendelse.

4.3. Personopplysningsforskriften § 1-3

I utredningens punkt 12.5.3.2 foreslås det at personopplysningsforskriften § 1-3 inntas i loven, fordi den utgjør en så vesentlig begrensning i lovens virkeområde.

Etter Datatilsynets vurdering er det avgjørende spørsmålet i tilknytning til forskriftens § 1-3 hvorvidt bestemmelsen skal oppheves eller ikke. Datatilsynets primære oppfatning er at § 1-3 bør oppheves slik at personopplysningsloven kommer til anvendelse også innenfor rettspleien, med mindre behandlingsmåten er særskilt regulert i lov, som vil være unntatt etter det generelle unntaket i personopplysningsloven § 5.

Datatilsynet har begrunnet dette på følgende måte i brev av 3. april 2009 til Fornyings- og administrasjonsdepartementet:

"Som nevnt ovenfor er Datatilsynets primære oppfatning at bestemmelsen bør oppheves slik at personopplysningsloven kommer til anvendelse også innenfor rettspleien – så sant ikke det er gitt særskilte bestemmelser på området. Bestemmelsen er kommentert i den kongelige resolusjon som ble gitt ifm. vedtakelsen av loven. Begrunnelsen som er gitt for denne er at unntak fra innsyns- og varslingsregler er nødvendig for ikke å umuliggjøre politiets etterretnings- og etterforskningsarbeid. Etter Datatilsynets vurdering bør imidlertid dette hensynet kunne ivaretas innenfor personopplysningsloven forutsatt at det gjøres enkelte presiseringer i denne. En opphevelse av bestemmelsen vil medføre at personopplysningsloven vil gjelde der annen lovgivning ikke sier noe om behandlingen, jf. lovens § 5. Dette vil danne

[6] EF-domstolens avgjørelse i sak C-101/01.

et sikkerhetsnett for behandling av personopplysninger på området. Når ny politiregisterlov trer i kraft vil særbestemmelser i denne uansett gå foran personopplysningsloven."

5. Geografisk virkeområde

Det er ikke foreslått noen endringer i personopplysningsloven § 4, og bestemmelsen er ikke omtalt i departementets høringsnotat. Imidlertid er bestemmelsen om personopplysningslovens geografiske virkeområde viet en del omtale i utredningen. Datatilsynet ser dette som et uttrykk for at departementet, på bakgrunn av den nevnte utredningen, ikke ser behov for klargjøring eller endring av innholdet i bestemmelsen. Datatilsynet har likevel enkelte merknader til uttalelsene i utredningen.

5.1. Etableringskriteriet

Slik bestemmelsen i personopplysningsloven § 4 første ledd fremstår i dag, kan man få inntrykk av at den norske personopplysningsloven kommer til anvendelse i alle tilfeller hvor den behandlingsansvarlige har et datterselskap eller en filial i Norge. Også enkelte uttalelser i forarbeidene til personopplysningsloven kan peke i retning av en slik lovforståelse:

"*Avgjørende er om den behandlingsansvarlige har tilstrekkelig tilknytning til Norge til å være etablert slik uttrykket forstås ut fra en alminnelig språklig forståelse. Dersom et utenlandsk selskap har et datterselskap som driver virksomhet i Norge, er tilknytningskravet åpenbart oppfylt slik at datterselskapet er etablert her. Det samme gjelder utenlandske selskapers filialer i Norge.*"[7]

Uttalelsen er kanskje ikke preget av den mest forbilledlige klarhet, jf. for eksempel henvisningen til at tilknytningskravet *åpenbart* må være oppfylt "slik at datterselskapet" er etablert i Norge. Et spørsmål som har oppstått i praksis, er hvorvidt den norske loven får anvendelse der den behandlingsansvarlige er et utenlandsk foretak, men har en filial i Norge, som overhodet ikke er involvert i den aktuelle behandlingen av personopplysninger. Tar man utgangspunkt i de synspunkter som er sitert over, kan konklusjonen bli at etableringskriteriet også må anses oppfylt i denne situasjonen. Datatilsynet har imidlertid uttalt seg i en annen retning, basert på andre uttalelser fra forarbeidene,[8] og på bakgrunn av ordlyden i direktivets artikkel 4 (1) a[9] – den behandlingsansvarlige vil bare være forpliktet etter norsk personvernlovgivning dersom filialen eller datterselskapet på et eller annet vis er *involvert* i den aktuelle behandlingen.[10]
De tvilsspørsmål om bestemmelsens rekkevidde som oppstår i praksis, lar seg etter Datatilsynets oppfatning løse ved en fortolkning av bestemmelsen i lys av de tilgjengelige rettskilder. Tilsynet er derfor enig i at det ikke er nødvendig med endringer i lovens ordlyd i denne sammenheng. Datatilsynet kan for øvrig vanskelig se at det finnes aktuelle alternativer til etableringslandsprinsippet som bestemmende kriterium for personopplysningslovens

[7] Ot.prp. nr. 92 (1998-99) side 106.
[8] Ot.prp. nr. 92 (1998-99) pkt. 4.5.3.
[9] "*the processing is carried out in the context of the activities of the controller...*"
[10] Jf. tilsynets saker 07/01522 og 07/00153

geografiske anvendelsesområde. Kriteriet står sentralt i personverndirektivet, jf. dets artikkel 4, og i fellesskapsretten for øvrig.

5.2. Hjelpemiddelbegrepet

Det ligger utenfor utredernes mandat å vurdere lovens § 4 annet ledd, men utredningen vier likevel et par sider til temaet. Bestemmelsen fastslår at selv om den behandlingsansvarlige ikke er etablert i EU/EØS-området, kan personopplysningsloven likevel komme til anvendelse, dersom den behandlingsansvarlige benytter *hjelpemidler* i Norge.

Det er ikke helt klart hva som ligger i hjelpemiddelbegrepet, men i forarbeidene til personopplysningsloven er det gitt enkelte eksempler. Et spørsmål som imidlertid ikke er besvart, og som også reises i utredningen, er hvorvidt dataprogrammer er omfattet av begrepet. I den senere tid har det dessuten pågått en debatt om hvorvidt såkalte "*cookies*", eller informasjonskapsler, er omfattet av bestemmelsens ordlyd. Artikkel 29-gruppen har gått langt i å antyde at svaret på dette spørsmålet er bekreftende.[11] Dermed vil det være nærliggende for Datatilsynet å tolke bestemmelsen i § 4 annet ledd i samsvar med dette, jf. EØS-avtalen artikkel 3.

Et alternativ vil imidlertid kunne være å eksplisitt avgrense mot denne typen "hjelpemidler" i lovteksten selv, eller eventuelt i andre rettskilder. Tilsynet ser i alle fall at det vil kunne føre til vanskelige tilstander dersom bruk av informasjonskapsler skulle resultere i at den norske loven kommer til anvendelse – dette vil i så fall utvide personopplysningslovens geografiske nedslagsfelt betraktelig, og bør følgelig vurderes av lovgiver.

5.3. Presisering av Datatilsynets kompetanse

Datatilsynet ser for øvrig ikke at det skulle være noe i veien for at Datatilsynets kompetanse presiseres i selve loven, jf. direktivets artikkel 28. nr 6.

---

[11] Se WP 148, "*Opinion 1/2008 on data protection issues related to search engines*", og WP 163 "*Opinion 5/2009 on online social networking*". For en mer detaljert gjennomgang, se WP 56 "*Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites*".

6. Ytringsfrihet og personvern

6.1. § 7 i personopplysningsloven

Personopplysningslovens § 7 har følgende ordlyd:

"For behandling av personopplysninger utelukkende for kunstneriske, litterære eller journalistiske, herunder opinionsdannende, formål gjelder bare bestemmelsene i §§ 13-15, § 26, §§ 36-41, jf. kapittel VIII."

Formålet med bestemmelsen er å avverge at personopplysningsloven i for stor grad begrenser ytringsfriheten. Både personvernet og ytringsfriheten er beskyttet av internasjonale menneskerettighetskonvensjoner. Rettighetene er sidestilte, det er ikke slik at man på generelt grunnlag kan fastslå at i situasjoner hvor det oppstår konflikt mellom dem skal den ene gis forrang over den andre.

Bestemmelsen implementerer artikkel 9 i EUs personverndirektiv som lyder:

"Processing of personal data and freedom of expression
Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."

Det følger av direktivet at skal gjøres unntak fra lovens anvendelsesområde i den grad det er nødvendig for å beskytte ytringsfriheten. Unntakene skal være basert på en proporsjonalitetsvurdering der hensynet til ytringsfriheten veies opp mot hensynet til den registrertes personvern.

I Schartum og Bygraves utredning konkluderes det med at § 7, slik den er utformet i dag, oppfyller Norges internasjonale forpliktelser. Dette tilsluttes i høringsnotatet. Datatilsynet deler denne oppfatningen.

Et annet spørsmål er hvorvidt bestemmelsen på en hensiktsmessig måte veier personvernhensyn og ytringsfriheten mot hverandre. For Datatilsynet er det avgjørende at ikke personvernet i for stor grad blir skadelidende.

Videre tilsier hensynet til forutberegnelighet at bestemmelsens ordlyd gir noen holdepunkter for å fastslå når ytringsfriheten skal slå gjennom. Det kan i den sammenheng tilføyes at også rettstekniske hensyn taler for en ordlyd som bidrar til klarhet og forutberegnelighet, selv om man neppe vil komme utenom vanskelige interesseavveininger i den enkelte sak.

6.2. Kort om bestemmelsens innhold

§ 7 regulerer lovens virkeområde. Når behandlingen av personopplysninger utelukkende skal tjene et kunstnerisk, litterært eller journalistisk, herunder opinionsdannende formål, gjelder kun et fåtall av lovens bestemmelser. Ordlyden er ment å fange opp den proporsjonalitetsavveining som direktivet legger opp til.

Bestemmelsene som likevel skal komme til anvendelse omfatter §§ 13-15 om informasjonssikkerhet, den nå opphevete § 26 om direkte markedsføring, bestemmelsene i kapittel VII om kameraovervåkning og kapittel VIII som regulerer Datatilsynets myndighet og sanksjonsmuligheter.

Datatilsynet har, med henvisning til § 7, vist forsiktighet med å fatte vedtak eller komme med føringer som begrenser ytringsfriheten. Datatilsynet har ikke sett det som sin oppgave å regulere kunstnerisk, litterær eller journalistisk virksomhet. At unntaket også omfatter behandling av personopplysninger som har et "opinionsdannende formål" har bidratt til ytterligere tilbakeholdenhet med å trekke grensene for hva som kan aksepteres i ly av ytringsfriheten. Det er dessuten tilsynets oppfatning at hensynene bak ytringsfriheten skal tillegges stor normativ tyngde.

6.3. Praktiske utfordringer

Siden personopplysningsloven ble vedtatt har den virkelighet loven skal regulere endret seg. Internetts utbredelse og økt kunnskap om de mulighetene det gir, har gjort enhver av oss i stand til å offentliggjøre våre ytringer. Gjennom denne kanalen kan enhver nå gjøre egne og andres personopplysninger tilgjengelige for allmennheten. Raske og sofistikerte søkemotorer på nettet gjør opplysninger lett tilgjengelige. Det kan stilles spørsmål ved om lovens § 7 på en tilstrekkelig måte tar høyde for denne utviklingen. Etter Datatilsynets syn har begrepet "opinionsdannende formål" bidratt til å gi unntaket et for omfattende nedslagsfelt.

Innehavere av rent private nettsider, eller en interessegruppes hjemmesider er ikke underlagt redaktøransvaret eller Vær Varsom-plakaten. I mylderet av slike nettsteder av ulike valører og med ulik agenda foreligger det i liten grad noen form for selvjustis som ivaretar hensynet til personvernet. Datatilsynet har sett flere eksempler på at personopplysninger publiseres på nettsider der det meddeles materiale som bør være beskyttet av ytringsfriheten, men hvor det i tillegg legges ut opplysninger om enkeltpersoner som i seg selv ikke på noe vis bidrar til å ivareta hensynene bak ytringsfriheten. I noen av disse eksemplene har opplysningene knyttet seg til identifiserbare barn, en sårbar gruppe med få muligheter til å ta til motmæle og ivareta egne interesser.

6.4. Forslag til utforming av bestemmelsen

Datatilsynet er av den oppfatning at hovedreglen i bestemmelsen som regulerer forholdet mellom personvern og ytringsfrihet, også i fremtiden bør være utformet som en bestemmelse som regulerer lovens anvendelsesområde. En bestemmelse som utelukkende sier at loven skal forstås i overensstemmelse med ytringsfriheten vil kunne undergrave hensynet til forutberegnelighet.

Videre anbefales det at begrepene kunstneriske, litterære og journalistiske formål videreføres. Det er disse begrepene som er benyttet i direktivets artikkel, og de berører dessuten kjernen i ytringsfriheten.

På bakgrunn av det som er sagt over slutter Datatilsynet seg til forslaget om å utelate "herunder opinionsdannede" fra bestemmelsen, slik departementet har lansert som et alternativ til ny ordlyd. Etter tilsynets vurdering utgjør formuleringen en svakhet ved dagens ordlyd fordi uttrykket "opinionsdannende" langt fra kan sies å ha et entydig innhold. Det har i praksis vist seg problematisk å sette grenser for hva begrepet skal omfatte. Videre vil en endring av ordlyden åpne for at § 7s anvendelsesområde kan begrenses noe i forhold til dagens praksis, slik at personopplysningsloven kan komme til anvendelse når det behandles personopplysninger uten at behandlingen kan sies å tjene ytringsfriheten.

Selv om tilsynet tar til orde for å utelate "herunder opinionsdannende" fra bestemmelsen er det like fullt klart at også andre aktører enn kunstnere, forfattere og den etablerte pressen må være beskyttet av ytringsfriheten. Muligheten til å målbære sine meninger og forsøke å skape oppslutning om disse må tilkomme enhver som måtte ønske det. Hensynet til en frie meningsbrytning tilsier dette.

Det vil utvilsomt være sammenhenger hvor den konkrete avveiningen mellom personvernet og ytringsfriheten vil by på utfordringer. Som påpekt over er det vanskelig å komme frem til en ordlyd som ivaretar begge hensynene uten at slike vanskelige avveininger vil måtte foretas, men det vil være en lite tilfredsstillende løsning å la personvernet bli skadelidende i enhver sammenheng hvor det kan anføres at ytringsfriheten kan spille inn. Datatilsynet ser det som sin oppgave å hegne om personvernet når den type spørsmål kommer på spissen og vil da måtte ta stilling til når personvernet bør få gjennomslag. Det antas at man i noen av de situasjonene vil kunne se hen til relevante presseetiske normer som er nedfelt i Vær Varsom-plakaten, for å finne holdepunkter for hvor langt ytringsfriheten rekker. Det pekes for eksempel på at det er god presseskikk å gi barn et utvidet vern.

Datatilsynet ser ikke nødvendigheten av å innføre et nytt annet punktum som helt generelt slår fast at loven ikke skal komme til anvendelse der dette vil være i strid med ytringsfriheten, slik det er foreslått. Etter tilsynets oppfatning er en slik bestemmelse helt overflødig all den tid ytringsfriheten er beskyttet av Grunnloven.

For å forenkle bestemmelsen, og unngå at bestemmelsens hovedinnhold tapes av syne, bør oppramsingen av de paragrafer som skal gjelde også i tifeller hvor ytringsfriheten skal ha forrang, begrenses. Henvisningen til den nå opphevede § 26 må naturligvis sløyfes. Det anbefales dessuten at man ikke lar kapittelet om kameraovervåkning få anvendelse.

Datatilsynet kan ikke se at disse reglene bør ha relevans når formålet med kameraovervåkningen *utelukkende* har et kunstnerisk, litterært eller journalistisk formål, eller av andre grunner bør være vernet av ytringsfriheten. Det kan uansett ikke være tvil om at i et tilfelle hvor en journalistisk virksomhet benytter overvåkningskameraer for å sikre sine økonomiske verdier vil overvåkningen omfattes av bestemmelsene i kapittel VII. Reglene om informasjonssikkerhet bør det imidlertid ikke gjøres unntak fra.

7. Krav til rettslig grunnlag for behandling av personopplysninger (§§ 8-11)

7.1. Rangering av de rettslige grunnlagene for behandling av personopplysninger

Datatilsynet deler ikke utredernes oppfatning av behovet for en rangering av de rettslige grunnlagene for behandling av personopplysninger i primære og sekundære grunnlag. Etter Datatilsynets oppfatning er det relativt klart at en tilfredsstillende lovhjemmel til å behandle personopplysninger går foran de øvrige behandlingsgrunnlagene. Problemstillingen har heller ikke kommet på spissen i tilsynets praksis.

Når det gjelder lovgivers intensjon om at samtykke vil være det foretrukne behandlingsgrunnlag, kan ikke Datatilsynet se at det er et særskilt behov for å klargjøre dette nærmere. Også på dette området er forvaltningspraksis klar, samtykke er utgangspunktet for behandling av personopplysninger.

Det er imidlertid slik at flere behandlinger av personopplysninger er basert på en avtale mellom partene, eller med hjemmel i personopplysningslovens § 8 bokstav f. Dette er ofte helt kurante behandlinger av personopplysninger, og det vil fremstå som omstendelig og uhensiktsmessig å måtte vurdere innhenting av samtykke i disse tilfellene. En konsekvens av en slik oppdeling kan også bli at den behandlingsansvarlige i for stor grad innhenter et samtykke som ikke tilfredsstiller de formelle kravene som stilles til en slik viljeserklæring. Datatilsynet tror heller ikke at det rokkes ved lovgivers intensjoner eller den enkeltes mulighet til å rå over egne opplysninger, at behandling av personopplysninger etter en nødvendighetsvurdering kan baseres på de alternative rettslige grunnlagene.

Særlig vurderer tilsynet det som lite hensiktsmessig med en oppdeling i primære og sekundære behandlingsgrunnlag dersom de sekundære rettslige grunnlagene kun kan gjøres gjeldende når det er "umulig eller uforholdsmessig vanskelig eller ressurskrevende" å oppfylle de primære. Eksempelvis vil det bære for langt av sted dersom en avtale mellom en bank og en kunde om inngåelse av en låneavtale må vurderes etter de primære behandlingsgrunnlagene før det kan konstateres at behandlingen kan skje for å gjennomføre en avtale med den registrerte, jf. dagens § 8 bokstav a.

Alternativt anser Datatilsynet det som et mulig alternativ å dele opp bestemmelsene i to ledd, hvor det av første ledd fremgår at behandling av personopplysninger kan skje med hjemmel i lov eller baseres på et samtykke fra den registrerte, mens annet ledd angir de øvrige behandlingsgrunnlagene. I den forbindelse kan også kravet til en tilfredsstillende lovhjemmel spesifiseres nærmere.

7.2. Øvrige endringer i § 8 og § 9

Datatilsynet har ikke sett behov for et behandlingsgrunnlag tilsvarende nåværende § 9 første ledd bokstav d for ikke-sensitive personopplysninger. I de tilfeller hvor den registrerte selv offentliggjør slike personopplysninger, vil det som hovedregel foreligge et rettslig grunnlag for behandling av opplysningene gjennom et samtykke eller etter personopplysningslovens § 8 f. Tilsynet er imidlertid ikke prinsipielt imot en slik regulering, dersom det fra lovgivers side antas at en slik regulering skaper større samsvar mellom bestemmelsene.

Datatilsynet savner derimot en bestemmelse tilsvarende lovens § 8 bokstav a også i § 9. Etter dagens regelverk er det ikke adgang til å behandle sensitive personopplysninger for å gjennomføre en avtale med den registrerte. Tilsynet anser dette som en svakhet ved reguleringen, all den tid slike avtaler er svært vanlige i det praktiske liv, eksempelvis innen interesseorganisasjoner, i bank- og forsikringsøyemed mv. Løsningen etter dagens lov er at den behandlingsansvarlige må innhente et samtykke i disse situasjonene. Et slikt "vikarierende" samtykke vil etter Datatilsynets vurdering ikke nødvendigvis oppfylle kravet til frivillighet, men behandlingen må like fullt antas å være rettmessig fra den behandlingsansvarliges side og heller ikke i strid med den registrertes interesser.

7.3. Sammenslåing av § 8 og § 9

Datatilsynet vurderer en sammenslåing av personopplysningslovens § 8 og § 9 som uheldig og utilrådelig. De sensitive personopplysningene er opplysninger som etter sin karakter antas å ha et større behov for vern enn øvrige personopplysninger. Det skal altså noe mer til for å behandle sensitive personopplysninger. At den behandlingsansvarlige tvinges til å vurdere både lovens § 8 og § 9 ved behandling av sensitive opplysninger kan bidra til å øke bevisstheten omkring skillet, og er etter tilsynets oppfatning i så måte positivt.

7.4. Grunnkrav til behandling av personopplysninger (§ 11)

Datatilsynet deler departementets oppfatning om at personopplysningsloven § 11 bør plasseres foran de bestemmelsene som oppstiller kravene til behandlingsgrunnlag, § 8 og 9. Lovens § 11 angir hvilke grunnkrav som stilles for behandling av personopplysninger, og bør særlig av pedagogiske hensyn plasseres så tidlig som mulig i loven. I tillegg fremstår det som lite logisk at et av grunnkravene som fremgår av bestemmelsen, jf den gjeldende § 11 bokstav a, påpeker at personopplysninger kun kan behandles når dette er tillatt etter de forutgående §§ 8 og 9. Datatilsynet tror ikke at en endret plassering vil medføre noen ulempe for brukerne av loven.

8. Den registrertes rettigheter mv. (§§ 16-28)

8.1. Rett til innsyn

Retten til innsyn er en grunnleggende personvernrettighet. Innsynsretten skal sette den enkelte i stand til å ivareta sine øvrige rettigheter etter loven. Dagens § 18 første ledd er en allmenn innsynsbestemmelse som gir enhver rett til innsyn i hva slags behandlinger av personopplysninger den behandlingsansvarlige foretar. Personopplysningslovens § 18 annet ledd er en individuell innsynsrett for den registrerte.

Datatilsynet støtter utredernes forslag om å klargjøre disse to typene av innsynsrettigheter ved en oppdeling i to paragrafer. Dette var også opprinnelig forslått i NOU 1997: 19, men ble ikke fulgt opp senere. Datatilsynet tror at en slik oppdeling i større grad enn i dag vil klargjøre de to formene for innsynrett, og forhåpentligvis fremheve den individuelle innsynsretten i større grad enn ved det litt bortgjemte annet ledd i § 18.

8.2. Informasjonsplikt (§ 19 og § 20)

8.2.1. Personopplysninger på avveie

I visse situasjoner har Datatilsynet savnet en klar hjemmel til å pålegge den behandlingsansvarlige en plikt til å informere de registrerte når deres personopplysninger har kommet på avveie. Grunnleggende personvernhensyn taler for at den behandlingsansvarlige burde ha en slik aktiv informasjonsplikt. Dersom ikke slik informasjon gis, står de registrerte uten mulighet til å ivareta eget tarv, herunder kreve erstatning eller gå til politianmeldelse.

Etter dagens regelverk gjelder det ingen klar informasjonsplikt i disse tilfellene, all den tid § 19 og § 20 bare gjelder når opplysningene hentes inn. Det er mulig at den behandlingsansvarlige kan sies å ha en generell ulovfestet skadebegrensingsplikt, som utløser en slik varslingsplikt overfor de registerte. Dette er imidlertid tvilsomt. Det er også tvilsomt i hvilken grad Datatilsynet selv kan, bør eller skal varsle de registrerte, for eksempel etter å ha mottatt en avviksmelding etter personopplysningsforskriftens § 2-6. Det er dessuten tvilsomt om Datatilsynet kan fatte vedtak med et pålegg etter lovens § 46 om at de registrerte skal varsles i et konkret tilfelle.

Datatilsynet foreslår derfor at det pålegges en uttrykkelig varslingsplikt for den behandlingsansvarlige, når det har funnet sted en uautorisert utlevering av personopplysninger. Tilsynet har ikke tatt stilling til om varslingsplikten bør begrenses til de tilfellene hvor konfidensialitet er nødvendig, tilsvarende plikten til å varsle etter forskriftens § 2-6.

Denne bestemmelsen bør hjemles i de alminnelige informasjonsbestemmelsene i loven, slik at også de alminnelige unntakene etter personopplysningslovens § 23 kommer til anvendelse.

8.3. Klargjøring av § 20 annet ledd

Etter Datatilsynets erfaring kan personopplysningslovens § 20 annet ledd bokstav a om unntak fra varslingsplikten når innsamlingen eller formidlingen av opplysningene er uttrykkelig fastsatt i lov, fremstå som vanskelig å forstå i praksis. Tilsynet ønsker derfor en omformulering av bestemmelsen, slik at det fremgår klart at hjemmelsgrunnlaget må inneholde tilstrekkelig informasjon til at den enkelte blir satt i stand til å ivareta sine øvrige rettigheter etter personopplysningsloven, jf. lovens § 19 og da særlig § 19 bokstav e. En slik omformulering antas ikke å gjøre noen endring i rettstilstanden, men fremstår som hensiktsmessig av pedagogiske hensyn.

8.4. Automatiserte avgjørelser (§ 22)

Departementet tar i punkt 10.6 opp behovet for endring av personopplysningslovens § 22 "for å være helt sikre på at direktivet er gjennomført korrekt". Det følger av nevnte bestemmelse at den registrerte har rett til informasjon om fullt automatiserte avgjørelser, mens direktivet også åpner for en overprøvingsmulighet av slike avgjørelser.

Etter Datatilsynets vurdering følger den etterlyste overprøvingsmuligheten allerede i dag av personopplysingslovens § 25, som gir den registrerte en rett til å kreve at en fullt automatisert avgjørelse av rettslig eller annen vesentlig betydning overprøves av en fysisk person. Datatilsynet legger derfor til grunn at direktivets artikkel 12 bokstav a tredje strekpunkt jf. artikkel 15 allerede er gjennomført i personopplysningsloven. Tilsvarende vurdering fremgår for øvrig av Ot prp nr 92 (1998-99) side 122, hvor det i tilknytning til personopplysningslovens § 25 heter at bestemmelsen "gjennomfører direktivet artikkel 15 nr 1." Datatilsynet anbefaler imidlertid at dette klargjøres ved at dagens § 25 følger direkte etter dagens § 22.

Til opplysning har bestemmelsene i personopplysningslovens § 22 og § 25 kun i svært begrenset grad kommet til anvendelse i Datatilsynets saksbehandling. Dette skyldes trolig en kombinasjon av uvitenhet om bestemmelsen og at det foreløpig ikke er vanlig med fullt automatiserte avgjørelser utenfor kredittopplysningsfeltet. Departementets forslag om innføring av konkrete saksbehandlingsregler i eksempelvis personopplysningsforskriften om hvordan en eventuell overprøving etter lovens § 25 skal gjennomføres, synes derfor ikke nødvendig.

9. Overføring av personopplysninger til utlandet

Nedenfor følger tilsynets kommentarer til departementets uttalelser og spørsmål i høringsnotatets punkt 5, om overføring av personopplysninger til utlandet, med særlig søkelys på overføring til såkalte "tredjeland", og til Schartum/Bygraves utredning kapittel 8 om samme tema.

9.1. Samtykke som vilkår for overføring til utlandet

Departementet har i høringsnotatet etterlyst høringsinstansenes synspunkter på spørsmålet om det bør inntas en presisering i loven om at et samtykke, som rettslig grunnlag for en tredjelandsoverføring, må være "*informert*". Etter den foreslåtte endringen, vil det følge av § 30 første ledd bokstav a at personopplysninger kan overføres til stater som ikke sikrer en forsvarlig behandling, dersom

"*den registrerte har samtykket i overføringen* ***(jf. § 6 annet ledd), og den registrerte forut for avgivelsen av samtykket er gjort oppmerksom på den særlige risiko som overføringen kan innebære***"

Bakgrunnen for forslaget er oppgitt å være "etter modell av den franske løsningen". Etter det Datatilsynet kan se, inneholder ikke den franske loven noen legaldefinisjon av begrepet *consentement,* som svarer til det norske begrepet *samtykke.*[12] Ei heller er det inntatt noen slik presentasjon i reglene om utenlandsoverføringer i den franske loven. Av CNILs veiledning om temaet, som det er vist til i utredningen, fremgår det imidlertid at samtykket må være informert, under henvisning til direktivets definisjon av et gyldig samtykke.[13] Ellers fremgår det av den franske lovens artikkel 69 første ledd at det eneste kriteriet til den registrertes samtykke, som grunnlag for overføring til tredjeland som ikke sikrer en forsvarlig behandling, er at dette er avgitt "*expressément*" – det vil si uttrykkelig eller utvetydig.

En slik presisering i det norske regelverket vil neppe være nødvendig. Grunnen til dette er at legaldefinisjonen av samtykkebegrepet i personopplysningsloven § 2 nr. 7 allerede inneholder en henvisning til at et samtykke skal være *informert.* Slik tilsynet ser det, kan det av legaldefinisjonen utledes et ufravikelig kriterium om at et samtykke bare er gyldig dersom den registrerte får et visst minstemål av informasjon om den behandling som hans eller hennes personopplysninger (skal) gjøres til gjenstand for. At dette må gjelde i alle sammenhenger hvor samtykkebegrepet benyttes i loven, fremgår direkte av ordlyden i § 2. De alminnelige bestemmelsene om den behandlingsansvarliges informasjonsplikt gir for øvrig langt på vei svar på spørsmålet om hvor langt plikten rekker, jf. lovens § 19 første ledd bokstav c og bokstav e.

Når det finnes få eksempler i Datatilsynets vedtakspraksis på at det overfor de behandlingsansvarlige understrekes at samtykke som overføringsgrunnlag krever oppfyllelse av flere kumulative vilkår, jf. § 2 nr. 7, kan dette bero på at samtykkebaserte utenlandsoverføringer i beskjeden grad gjøres kjent for tilsynet. Dette kan også ha

---

[12] Jf. Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004)
[13] http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/Guide-tranfertdedonnees.pdf

sammenheng med at Datatilsynet er tilbakeholdent med å anbefale at samtykke benyttes i nærværende sammenheng, jf. følgende uttalelser på www.datatilsynet.no: "*Et gyldig samtykke må være avgitt frivillig og kan på ethvert tidspunkt trekkes tilbake, jf. § 2 nr. 7. Samtykke vil derfor ofte være lite egnet som grunnlag for overføring til utlandet*". Uttalelsen er blant annet basert på Artikkel 29-gruppens arbeidsdokument om en ensartet fortolkning av artikkel 26 (1), der det også tas til orde for at unntakene i direktivets artikkel 26 (1) må anvendes restriktivt.[14]

På den annen side vil tilsynet tilføye at det nok i praksis hersker en viss tvil blant de behandlingsansvarlige om hvor omfattende informasjonsplikten er i slike sammenhenger. Tilsynet er derfor enig i at de aktuelle lovbestemmelsene kan sammenfattes og forklares nærmere, men ser på dette som en oppgave som naturlig hører inn under Datatilsynets rådgivende og veiledende funksjon, jf. personopplysningsloven § 42 tredje ledd nr. 6.

Et annet spørsmål er om det burde fremgå klarere av lovteksten at samtykket må være spesifikt for en bestemt overføring av personopplysninger. Direktivet påpeker at samtykket må gjelde den *forestående* eller *planlagte* overføringen, jf. den engelske direktivtekstens henvisning til "*the proposed transfer*".[15]

9.2. Forholdet til EU-kommisjonens beslutninger

Datatilsynet er av den oppfatning at ordningen kan opprettholdes slik den er i dag. Det vil være lite å vinne på at forskriftens § 6-1 flyttes til loven, ikke minst fordi bestemmelsen først og fremst må leses som en pliktregel som har tilsynsmyndigheten som adressat. Det kan i den anledning vises til at det på Datatilsynets nettsted er opplyst at personopplysninger kan overføres til stater som er godkjent av EU uten hinder av begrensningene i lovens § 29 og 30.

9.3. Meldeplikt

Datatilsynet er enig med departementet i at innføring av en utvidet meldeplikt for utenlandsoverføringer vil føre med seg få gevinster, og at en slik regel er uhensiktsmessig. Dersom overføringen samtidig utgjør en utlevering av personopplysninger fra en behandlingsansvarlig virksomhet til en annen, utløses dessuten meldeplikten for den behandlingsansvarlige som utleverer opplysningene. Denne situasjonen skiller seg altså ikke fra en utlevering av personopplysninger til aktører innenfor landets grenser. I en slik melding skal det alltid opplyses hvorvidt opplysningene vil bli utlevert til tredjeland, jf. lovens § 32 første ledd bokstav h. Det er da også inntatt en egen rubrikk for denne typen informasjon i meldeskjemaet, se skjemaets punkt 7.

Dersom den behandlingsansvarlige på et senere tidspunkt, det vil si etter at melding er sendt og det er varslet om at det ikke skal utleveres/overføres opplysninger til tredjeland, beslutter å overføre opplysningene til en annen behandlingsansvarlig virksomhet, må dette i så fall regnes som en ny behandling, som eventuelt utløser ny meldeplikt.

En overføring av personopplysninger kan også finne sted når mottakeren i utlandet er en databehandler, jf. EU-kommisjonens beslutning av 27 desember 2001 (2002/16/EF). På

---

[14] Se WP 114 s. 12.

[15] Lignende formuleringer går igjen i den franske og den svenske teksten, jf. hhv. "*[le] transfert envisagé*" og "*den planerade överföringen*". Den danske og den tyske språkversjonen ser ut til å mangle en slik presisering

samme måte som i de nasjonale tilfeller, vil ikke en slik overføring utløse meldeplikt, sml. personopplysningsloven § 15.

9.4. Internettpublisering

Publisering av personopplysninger på Internett innebærer en risiko for at opplysningene kan aksesseres fra alle kanter av verden. Enkelte uttalelser i forarbeidene til personopplysningsloven, gi da også temmelig langt i å fastslå at en hver internettpublisering av personopplysninger samtidig automatisk måtte regnes som en overføring til utlandet. Etter Lindqvist-saken, endret oppfatningen seg. Domstolen presiserte blant annet at det ikke kan antas at fellesskapslovgiver har tilsiktet at personverndirektivets bestemmelser om overføring skulle omfatte fremtidige situasjoner som denne. Datatilsynet er enig i enkelte av Domstolens synspunkter, ikke minst fordi det ville få konsekvenser som det er vanskelig se rekkeviddene av dersom en hver internettpublisering skulle utløse plikter etter reglene om overføring til utlandet. På den annen side kan det fremstå som urimelig dersom en legger an det motsatte syn, nemlig at en hver internettpublisering skulle gå klar av disse reglene. Når man har fastslått at en *målrettet overføring* til utlandet, for eksempel via e-post, er omfattet av reglene, ville det virke direkte underlig om man kunne unngå det samme regelverket ved å legge de samme opplysningene ut på det åpne Internett i stedet. Av disse årsakene, tror tilsynet det kan være klokt å avvente nærmere regulering av spørsmålet, og i stedet la de nasjonale myndigheter beholde den skjønnsmargin som eksisterer i dagens lovgivning.

9.5. Hvem er forpliktet til å foreta vurderingen i § 29 annet ledd?

I høringsnotatets punkt 5.1, hvor det redegjøres for dagens rettstilstand vedrørende overføring av personopplysninger til utlandet, er det uttalt:

" For andre tredjeland må det foretas en konkret forsvarlighetsvurdering, jf. § 29 annet ledd hvor det angis hvilke momenter som skal vektlegges ved denne vurderingen. Forsvarlighetsvurderingen forutsetter kunnskap om mottakerlandets personvernregulering. Det er den behandlingsansvarlige selv som må skaffe seg denne kunnskapen, men i praksis vil det kunne være naturlig å søke råd hos Datatilsynet."

Tilsynet ønsker å gjøre departementet oppmerksom på at rettskildebildet gjør at det kan settes spørsmålstegn ved om dette er en korrekt gjengivelse av dagens rettstilstand. For det første er ordlyden i seg selv uklar med hensyn til hvem som skal stå for den omtalte vurderingen. For det andre fremgår det av NOU 1997:19 at det er Datatilsynet som er tiltenkt rollen som subjekt i bestemmelsen, idet det er uttalt at "[...] *Datatilsynet kan se hen til ytterligere momenter i vurderingen av om beskyttelsesnivået er tilstrekkelig*".[16]

Riktignok finnes det en enkelt uttalelse i Ot.prp. nr 92 (1998-99) som trekker i en annen retning:

"*Det er i utgangspunktet den behandlingsansvarlige selv som må vurdere om det landet som opplysningene skal overføres til vil sikre en forsvarlig behandling, jf punkt 10.5. Datatilsynet vil imidlertid ha en sentral veiledningsfunksjon, jf § 42 tredje ledd nr 6 i lovforslaget.*"

[16] Se utredningens pkt. 16.4.2.3.

Det siste harmonerer etter Datatilsynets mening dårlig med direktivets utgangspunkt i artikkel 25 (1), som bestemmer:

"Medlemsstaterne fastsætter bestemmelser om, at videregivelse til et tredjeland af personoplysninger, der gøres til genstand for behandling, eller som skal gøres til genstand for behandling efter videregivelsen, kun må finde sted, hvis det pågældende tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, og forudsat at de nationale bestemmelser, der vedtages til gennemførelse af direktivets øvrige bestemmelser, overholdes.

Ansvaret for å påse at personopplysninger kun overføres til tredjeland som sikrer et tilstrekkelig beskyttelsesnivå, hviler altså i utgangspunktet på den enkelte medlemsstat. EU-kommisjonen har da også uttalt følgende om implementeringen av direktivet Artikkel 25 i de ulike medlemsstatene:[17]

"Den fremgangsmåde, som visse medlemsstater har valgt, og hvor det er den registeransvarlige, der skal vurdere, hvorvidt den beskyttelse, som modtageren yder, er tilstrækkelig, således at de offentlige myndigheder eller den nationale tilsynsmyndighed kun har meget begrænset kontrol med datastrømmen, synes ikke at være i overensstemmelse med den forpligtelse, der pålæggesmedlemsstaterne i henhold til artikel 25, stk. 1."

Også Artikkel 29-gruppen har gitt uttrykk for at det er de nasjonale myndigheter som er nærmest til å foreta en slik vurdering. Hvorvidt denne myndigheten skal være Datatilsynet er imidlertid ikke helt entydig:

"Direktivet pålægger således medlemsstaterne at sikre, at der ikke overføres personoplysninger til et tredjeland, medmindre det yder et tilstrækkeligt beskyttelsesniveau, og det bestemmes i direktivet, at vurderingen af, hvorvidt beskyttelsesniveauet er tilstrækkeligt, skal ske på grundlag af samtlige forhold. Det præciseres imidlertid ikke i direktivet, om en bestemt myndighed skal foretage denne vurdering af databeskyttelsesniveauet i tredjelandene. Denne opgave kan således i henhold til medlemsstaternes nationale lovgivning påhvile de nationale databeskyttelsesmyndigheder, som eventuelt skal godkende overførslen af personoplysninger til tredjelande."[18]

Datatilsynet er ikke enig i at det bør være opp til den behandlingsansvarlige å foreta denne vurderingen. De vurderinger som skisseres i personopplysningsloven § 29 annet ledd og i direktivets artikkel 25 (2), kan være svært sammensatte, og fordrer trolig grundige kunnskaper om så vel rettslige som faktiske forhold i det aktuelle tredjelandet.[19]

Tilsynet er for øvrig bekymret for at objektiviteten i den behandlingsansvarliges eventuelle vurderinger etter bestemmelsen i praksis vil kunne bli svekket. En utenlandsoverføring basert på en slik forhåndsvurdering vil heller ikke bli bekjentgjort for tilsynsmyndigheten på annen måte enn gjennom en eventuell melding. Følger man denne tilnærmingen, ville det med andre ord kunne føre til ytterligere mørketall på området. Dessuten ville det bli umulig for

---

[17] *BERETNING FRA KOMMISSIONEN – Første beretning om gennemførelsen af databeskyttelsesdirektivet (95/46/EF). KOM(2003) 265 endelig.*

[18] WP 114 side 4.

[19] Som et eksempel på dette, kan det vises til Kommisjonens beslutning om godkjenning av Argentina som trygg mottakerstat med tilhørende uttalelse 4/2002 fra Artikkel 29-gruppen om databeskyttelsesnivået i landet, tilgjengelig via *http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.*

Datatilsynet å oppfylle eventuelle forpliktelser på Norges vegne etter personopplysningsforskriften § 6-1, jf. direktivets Artikkel 25 (4), som forutsetter at medlemsstatene er forpliktet til å hindre en hver overføring til land som ifølge Kommisjonen ikke sikrer et tilstrekkelig beskyttelsesnivå.

På denne bakgrunn ber tilsynet om at departementet vurderer hvorvidt det er formålstjenlig å innta i lovbestemmelsen en presisering av om det er Datatilsynet, eventuelt en annen myndighet, som skal foreta den i § 29 omtalte vurderingen, eller om det skal være opp til den behandlingsansvarlige – eventuelt i samråd med Datatilsynet – å vurdere de forhold som det ifølge bestemmelsen *"bl.a. [skal] legges vekt på"*.

10. Melde- og konsesjonsplikten

I det følgende vil Datatilsynet kommentere de fremlagte forslag til endringer av personopplysningsloven kapittel VI, jf. høringsnotatets punkt 6, og utredningens kapittel 9. Tilsynet har tatt utgangspunkt i de to lovforslagene, men de fleste merknadene er knyttet til det radikale forslaget.

10.1. Gjeldende rett og utredernes forslag

Lovens utgangspunkt er i dag at *sensitive personopplysninger* ikke kan behandles uten konsesjon – med andre ord eksisterer det et alminnelig forbud mot behandling av slike personopplysninger. Det finnes imidlertid en rekke unntak fra denne hovedregelen, både i personopplysningsloven selv, og i personopplysningsforskriften.

Utredningens radikale forslag går i korte trekk ut på å oppheve dagens hovedregel om konsesjonsplikt, som er knyttet til behandlingen av sensitive personopplysninger. I stedet lanseres et forslag om en ny hovedregel som fastsetter at det positivt, og etter en *"konkret vurdering"*, skal angis hvilken *"behandling av personopplysninger"* som krever konsesjon, jf. forslagets § 33.

I utredningen foreslås det altså at det ikke lenger skal eksistere et generelt forbud mot å behandle sensitive personopplysninger, og at koblingen mellom sensitive personopplysninger og konsesjonsplikt fjernes. Lovens kapittel om melde- og konsesjonsplikt er med andre ord blant de områder i loven som er gjenstand for de mest omfattende endringene.

10.2. Generelle kommentarer og alternativt forslag

Datatilsynet har merket seg bakgrunnen for departementets ønske om å innsnevre omfanget av konsesjonsplikten:

"Erfaringer fra Datatilsynet tilsier at dagens konsesjonsplikt er for omfattende og fører til en lite hensiktsmessig bruk av tilsynets ressurser. Departementet ber om at det utformes ett eller flere forslag som fører til en klar reduksjon av antallet konsesjonssaker. Det må vurderes om en mer målrettet tilnærming kan gi en bedre løsning enn dagens konsesjonsplikt. For eksempel bør det vurderes om det er mulig å utforme konsesjonsplikten slik at den bare

gjelder for nærmere bestemte behandlingsformer som typisk lett kan krenke personvernet." [20]

I utredningen er det også uttalt at *"Det er i utgangspunktet grunn til å understreke at vi ikke har gjort noen systematisk undersøkelse av Datatilsynets arbeidsmetoder og prioriteringer, og at dette heller ikke inngår i mandatet for denne utredningen."*[21]

Formålet med konsesjonsordningen er først og fremst å sikre at behandlinger av personopplysninger som er særlig inngripende eller belastende vis-à-vis de ulike personverninteressene, ikke settes i gang uten forhåndsvurdering.[22] Fra personregisterloven av 1978 og frem til i dag, har man vært vitne til at lovgiver har fjernet seg fra forhåndskontroll som det primære tiltak for oppsyn med overholdelsen av regelverket, til dels i kombinasjon med tilsvarende utvidelser i ulike *etterkontrollerende* tiltak.[23] Slike tiltak kan være utvidet meldeplikt, utstrakt veiledingsvirksomhet og stedlige kontroller av virksomhetene. I tillegg kan tilsynets sanksjonsmidler nevnes, og innføring av nye materielle regler har også blitt fremført som et alternativ, jf. sitatet nedenfor.[24]

En av årsakene til denne utviklingen har vært knyttet til Datatilsynets kapasitet, noe som må sees i sammenheng med overgangen fra *personregister* til *elektronisk behandling* som lovgivningens sentrale begreper i 2001. Følgende passasje er hentet fra NOU 1997:19:[25]

"Et hovedspørsmål i Føyenutredningen var hvilken reguleringsform man burde bygge på i framtiden. Føyen mente at det beste alternativet for regulering av bruk av personopplysninger var det som var lovfestet i personregisterloven, men at en slik ordning forutsatte en vesentlig økning av Datatilsynets bemanning. Hvis dette ikke skjedde, mente Føyen at man burde gå bort fra konsesjonsbehandlingen for personregistre og i stedet ha flere materielle normer i loven. Datatilsynet burde i så fall gjøres til et organ med flere ombudsliknende oppgaver og en viss myndighet til å gi forbud og påbud."

Den opprinnelige begrunnelsen for å innskrenke konsesjonsinstituttet hadde med andre ord sammenheng med at man så for seg en heving av antallet konsesjonssøknader, som følge av den digitale revolusjon. Sett i lys av en slik utvikling, som ville medføre konsesjonsplikt for samtlige elektroniske behandlinger av så vel sensitive som ikke-sensitive opplysninger, ville man uten tvil måtte gi Føyen rett i at tilsynet raskt ville få kapasitetsproblemer.

Spørsmålet som departementet stiller, er hvilke virkemidler som i fremtiden vil være best egnet til å legge til rette for en hensiktsmessig og fornuftig ressursbruk i Datatilsynet. Et annet spørsmål som det er viktig å reise, er om ressurs- eller kapasitetsargumentet fremdeles gjør seg gjeldende med samme styrke. Spørsmålene drøftes nærmere i det følgende, etter en oppsummering av tilsynets anbefalinger:

---

20 Se mandatet gjengitt i utredningen på side 104, jf. også departementets høringsnotat side 47.
21 På samme sted i utredningen.
22 Se NOU 1997:19 avsnitt 12.5.5.1.
23 Se for eksempel NOU 1997:19 avsnitt 1.2.2.
24 ibid.
25 Avsnitt 12.4 side 104.

Datatilsynets konklusjon er at hovedregelen om konsesjonsplikt bør beholdes slik den er, *men* at det samtidig bør innføres en skjønnsmessig adgang for tilsynet til å dispensere fra konsesjonsplikten. En slik dispensasjonshjemmel kan tilføyes lovens § 33, for eksempel i form av et nytt ledd. Bestemmelsen kan beskrives som en *speilvendt* variant av dagens annet ledd, som gir tilsynet adgang til å bestemme at behandling av andre opplysninger enn de sensitive, også skal underlegges konsesjonsplikt. På denne måten kan det sikres at konsesjonsplikten (på sikt) bare omfatter "*behandlingsformer som typisk lett kan krenke personvernet*", slik departementet formulerer det i mandatet til utrederne. Resultatet vil bli at ulempene ved dagens konsesjonsordning elimineres, samtidig som fordelene ved systemet bevares.

10.3. Uheldige sider ved å innskrenke konsesjonsplikten

En ytterligere innsnevring i konsesjonsplikten begrunnes også i dag med andelen av tilsynets ressurser som er relatert til konsesjonsplikten. Datatilsynet mener imidlertid dette *kapasitetsargumentet* ikke lenger kan ha den samme tyngde som tidligere.

For det første kan det settes spørsmålstegn ved om en reduksjon i antallet konsesjonssaker i realiteten vil føre til en mer fornuftig ressursforvaltning i Datatilsynet, all den tid tomrommet som etterlates må fylles med et av de øvrige tilgjengelige virkemidlene. Det finnes få holdepunkter for å anta at for eksempel alminnelig saksbehandling eller andre former for etterkontroll, vil legge beslag på færre timer enn konsesjonsbehandling. Selve konsesjonsbehandlingen er ikke nødvendigvis mer krevende enn andre oppgaver som innebærer regelanvendelse og subsumpsjon.

Dersom ønsket er økt etterkontroll i form av stedlige kontroller, som kompensasjon for innskrenket konsesjonsplikt, må det pekes på at det både vil være ressurskrevende og kostnadsdrivende å gjennomføre landsdekkende observasjoner av virksomhetenes behandling av personopplysninger. I noen tilfeller er slik stedlig kontroll nødvendig og hensiktsmessig, mens i andre tilfeller vil det være tilstrekkelig med forhåndskontroll. Datatilsynet bør ha anledning til fritt å kunne ta stilling til hvordan ressursene skal fordeles på de ulike virkemidlene.

En annen grunn til at kapasitetsargumentet ikke kan fremføres med samme styrke som tidligere, er at en vesentlig andel av sakene som tidligere utløste konsesjonsplikt, nå er underlagt *helseforskningsloven*.[26] Loven, som trådte i kraft den 1. juli i år, medfører blant annet at saker som angår medisinsk og helsefaglig forskning ikke lenger skal behandles av Datatilsynet. Disse sakene skal nå utelukkende vurderes av en regional etisk forskningskomité. Dette betyr at en betydelig del av tilsynets kapasitet nå er frigjort.

10.3.1. Andre fordeler ved konsesjonsbehandling

Konsesjonsbehandling kan også fungere som en sikkerhetsforanstaltning overfor behandlinger av personopplysninger som kan vise seg å være svært personvernkrenkende. Gjennom konsesjonsordningen må Datatilsynet ta stilling til hvorvidt behandlingen skal kunne utføres,

---

[26] Lov om medisinsk og helsefaglig forskning 20. juni 2008 nr. 44.

idet det sees hen til de registrertes interesser, personopplysningene som behandles og omstendighetene for øvrig. En grundig forhåndsvurdering vil med andre ord kunne være den eneste effektive garanti mot at krenkende behandlinger iverksettes, for derigjennom å avverge eventuelle uopprettelige skader. Konklusjonen er at store "personvernkatastrofer" kan unngås gjennom forhåndskontroll.

I forarbeidene til personopplysningsloven heter det:

"Under høringsrunden gikk mange instanser inn for å beholde konsesjonsordningen. Det ble bl a pekt på at konsesjonsordningen sikrer en grundig forhåndsvurdering av registrene, at den gir impulser til kritisk vurdering av bruken av personopplysninger og at publikum får tillit til registerførerne (jf Ot prp nr 34 (1986-87) s 11 – 12)."[27]

I tillegg til at den grundige forhåndsvurderingen fremheves som sentral, anføres det altså også at hensynet til den behandlingsansvarlige må vektlegges. At en innsnevring av konsesjonsplikten i seg selv kan lede til et lavere bevissthetsnivå blant de behandlingsansvarlige, er etter Datatilsynets oppfatning sannsynlig – med mindre det innføres kompenserende tiltak med tilsvarende effekt.

Andre fordeler med konsesjonsinstituttet, slik det eksisterer i dag, er den fleksibiliteten det gir, først og fremst til fordel for tilsynsmyndigheten, men også for den behandlingsansvarlige og de registrerte. Det siktes her til at gjeldende konsesjoner kan endres i enkeltvedtaks form, etter hvert som de ulike behovene manifesterer seg. De behandlingsansvarlige og de registrerte gis således en nokså umiddelbar mulighet til å påvirke det regelverk som angår dem selv, gjennom innspill direkte overfor Datatilsynet om hva som vil være adekvate løsninger, sett fra de ulike ståsted. Prosessen vil dermed ivareta grunnleggende demokratiske hensyn, samtidig som eventuelle endringer kan gjennomføres på en langt mer effektiv måte enn gjennom endring av lov eller forskrift.

10.4. Visse ulemper forbundet med konsesjonsordningen

Summarisk behandling av likelydende konsesjonssøknader til samme behandlingsformål forekommer imidlertid. I de såkalte Bokart-sakene, som tilsynet har kommet til at er konsesjonspliktige, finnes det sågar et ferdig utfylt søknadsskjema på internettsidene til Husbanken. Slik får den behandlingsansvarlige en enkel jobb, og mange av de formålene som konsesjonsinstituttet skal ivareta, som for eksempel målsetningen om å høyne bevissthetsnivået om personvern hos den behandlingsansvarlige, vil ikke ivaretas.[28]

I forarbeidene til personopplysningsloven er det anført:

"De av høringsinstansene som gikk inn for en innsnevring av eller avskaffelse av konsesjonsordningen, begrunnet dette med at det ville være en forenkling."[29]

---

[27] Jf. NOU 1997:19 avsnitt 1.2.2.

[28] Situasjonen ser ut til å være kjent, jf. mandatbeskrivelsen under kapittel 9 i utredningen.

[29] NOU 1997:19 avsnitt 12.4.

Hva denne forenklingen i så fall skulle innebære forblir usagt, og eventuelt til fordel for hvem.

I forarbeidene er det videre gitt uttrykk for at man ikke bør erstatte konsesjonsbehandlingen med ytterligere bestemmelser i lovgivningen, fordi "slike regler lett ville bli for *vage* og *generelle*, samtidig som de ikke ville passe for alle typer virksomheter."[30]

Datatilsynets inntrykk er at argumentene for å begrense konsesjonsplikten gjennom å snu hovedregelen slik at ikke er overbevisende. Under tidligere lovrevisjon er det vist til ønsker om "forenkling" og frigjøring av kapasitet, uten at det er redegjort for hvilke gevinster en kan se for seg som en følge av disse tiltakene. Tilsynet opplever at historien gjentar seg, ettersom det også i denne omgang i stor utstrekning er vist til Datatilsynets kapasitet, og hensynet til forenkling av regelverket.

Til slutt gjentas et generelt poeng: Større endringer i reguleringsformen vil i seg selv medføre merarbeid for alle som er vant til å håndtere det eksisterende regelverket. Dette skulle trekke i retning av at man er tilbakeholden med å foreta større endringer, så lenge det er usikkert om den nye ordningen faktisk vil innebære forbedringer eller fordeler for pliktsubjekter, rettighetshavere, rettsanvendere eller tilsynsmyndighet. I tråd med dette synspunktet, kan det vises til nok en uttalelse fra forarbeidene til personopplysningsloven:

"Justisdepartementet kom til at man ikke burde foreslå å gå bort fra konsesjonsordningen for personregistre. Det ble lagt vekt på konsesjonsordningens fordeler, og på at Datatilsynet selv ønsket å beholde en konsesjonsordning uavhengig av om personalressursene ble økt. Endelig ble det vektlagt at større endringer i reguleringsformen ville medføre atskillig merarbeid, og at dette tilsa varsomhet med å foreta større endringer så lenge det var usikkert om den nye ordningen ville innebære en bedring."

10.5. Merknader til de enkelte endringsforslagene – radikalt forslag

Ny hovedregel om meldeplikt – forslagets § 31
Datatilsynet har ingen konkrete merknader til dette forslaget, utover det som er sagt under avsnittene om forslagets §§ 33 og 33 a, om rett til å kreve konsesjonsbehandling, og til de generelle merknadene.

Fornyet melding og varsel – forslagets § 31a
Datatilsynet har ingen konkrete merknader til forslaget, men viser til det som er sagt under avsnittet om Datatilsynets rett til å kreve konsesjonsbehandling, og til de generelle merknadene.

---

30 ibid.

Meldingens og varselets innhold – forslagets § 32
Datatilsynet har ingen konkrete merknader til forslaget, utover det som er sagt under avsnittene om forslagets §§ 33 og 33 a, om rett til å kreve konsesjonsbehandling, og til de generelle merknadene.

Datatilsynets rett til å kreve konsesjonsbehandling – forslagets § 33
Datatilsynet vil ikke anbefale departementet å følge opp det radikale forslaget om å gi Datatilsynet en *rett til å kreve konsesjonsbehandling* i det enkelte tilfellet. En slik løsning vil i så fall innebære at tilsynet må forhåndsvurdere alle innkommende meldinger med tanke på konsesjonsplikt, jf. forslaget om å kompensere med en utvidelse av meldeplikten. Antallet nye meldinger som registreres i Datatilsynets database hvert år er allerede meget høyt, og vil trolig øke dersom spekteret av meldepliktige behandlinger utvides. Av tilsynets årsmeldinger fra årene 2005 tom. 2008, fremgår det at det under dagens ordning registreres om lag 3000 meldinger i året[31]. Skulle alle disse meldingene forhåndsvurderes med tanke på senere konsesjonsbehandling, ville den manuelle sorteringen i seg selv sannsynligvis legge beslag på langt mer omfattende ressurser enn hva selve konsesjonsbehandlingen gjør i dag. Eventuelle gevinster i form av frigjorte ressurser, vil man følgelig måtte se langt etter.

Det er i utredningen skissert en prosedyre som automatisk skal kunne sortere ut meldinger som inneholder henvisninger til behandlinger av personopplysninger som vil kunne ha en særlig negativ virkning for den enkeltes personvern. Når det samtidig er fremmet forslag om at tilknytningen mellom konsesjonsplikt og sensitive personopplysninger skal fjernes, er det vanskelig å forstå hvilke kriterier i meldeskjemaet – foruten nettopp de sensitive personopplysningene – som skal føre til at en enkelt sak vekker tilsynsmyndighetens særskilte oppmerksomhet. Dersom det er behandlingen av sensitive opplysninger som skal utløse det automatiske "varsel", eller lignende, vil man etter tilsynets oppfatning oppnå svært lite – i praksis ville man være tilbake i dagens ordning, dog supplert med en mulighet for tilsynet til å ikke beslutte konsesjonsbehandling.

De registrertes rett til å kreve konsesjonsbehandling – forslagets § 33a
Datatilsynet anbefaler ikke at det innføres en slik regel. Forslaget fremstår som nokså fremmed i en rettslig kontekst. Etter tilsynets oppfatning er det uheldig at utenforliggende og totalt uberegnelige faktorer skal kunne få innflytelse over tilsynets ressursbruk. Som utrederne har understreket fremstår de tall som er angitt i endringsforslaget som nokså tilfeldige.

Konsesjonsplikt i henhold til forskrift – forslagets § 33b
Datatilsynet har ingen innvendinger mot forslaget om å bevare særregler i forskrift om konsesjonsplikt for særlige bransjer eller behandlingsformer. Tilsynet er for øvrig enig i at det samlede regelverket om melde- og konsesjonsplikt kan fremstå som uoversiktlig. Flere av unntaksbestemmelsene fremstår for øvrig som uklare i seg selv, både med hensyn til rekkevidde og utforming generelt. §§ 7-11 og 7-16 er etter tilsynets skjønn to eksempler på dette.

---

[31] I 2005 var antallet meldinger 2953, i 2006: 3019, 2007: 2952 og 2008: 2910, se årsmeldingene på http://www.datatilsynet.no/templates/Page____718.aspx

Det generelle inntrykket er at det legges ned mye tid i å vurdere rekkeviddene av de enkelte unntak. Først og fremst antar vi at dette gjelder blant de behandlingsansvarlige eller deres representanter, men det samme kan anføres i noen grad også for Datatilsynets del. Selve vurderingen av om en bestemt behandling av personopplysninger utløser meldeplikt, vil kunne være mer tid- og ressurskrevende enn å sende melding til Datatilsynet, først som sist. Spørsmålet blir da om man har noe å vinne ved å innvilge unntak fra meldeplikten. Dersom vurderingsprosessen hos den behandlingsansvarlige medfører at bevissthetsnivået ved behandling av personopplysninger høynes, kan dette være et argument for at meldeplikten bevares uinnskrenket. Dersom tids- og ressursbruken med rette kan karakteriseres som et problem, er tilsynets oppfatning at dette neppe kan rubriseres som alvorlig.

Unntak fra konsesjonsplikt når behandlingen har hjemmel i lov – forslagets § 33c
Endringene som er foreslått lyder:
"*Datatilsynet kan ikke nekte behandling av personopplysninger eller stille vilkår for at slik behandling kan skje dersom dette vil stride mot bestemmelse i lov eller forskrift gitt i medhold av slik lov. Det samme gjelder behandling av personopplysninger som er utvetydig forutsatt i nevnte lover eller forskrifter.*

Innenfor gjeldende lov- og forskriftsbestemmelser som nevnt i forrige ledd, kan Datatilsynet likevel treffe vedtak om supplerende tiltak som åpenbart er nødvendig for å ivareta personvernet, og som ikke hindrer realisering av lovens eller forskriftens formål."

Endringsforslaget introduserer en ny standard, hvoretter Datatilsynet er forpliktet til å akseptere en hver "*behandling av personopplysninger som er utvetydig forutsatt i nevnte lover eller forskrifter*". Tilsynet anser at denne oppmykningen av hjemmelskravet kan føre med seg uheldige konsekvenser, ikke minst for de registrerte, ettersom rettstilstanden vil bli langt mindre forutberegnelig. Videre er det en opplagt konsekvens er at det vil kunne samles inn atskillig større mengder personopplysninger i flere situasjoner, på bakgrunn av den behandlingsansvarliges egen fortolkning av et vagt og utydelig regelverk. I kjølvannet av dette er det lett å se for seg at det vil kunne oppstå vanskelige stridsspørsmål om hvorvidt det foreligger en "*utvetydig forutsetning*", et uttrykk som etter tilsynets oppfatning i seg selv består av gjensidig motstridende elementer.

Endringsforslaget tar heller ikke høyde for at hjemmelskravet i visse tilfeller bør skjerpes, for eksempel der den behandlingsansvarlige har til hensikt å behandle sensitive personopplysninger. Behandling av for eksempel helseopplysninger basert på forutsetninger i lov- eller forskriftstekst, vil etter Datatilsynets mening stride mot grunnleggende prinsipper, og mot den allmenne rettsoppfatning.

Datatilsynet kan for øvrig ikke se at dette endringsforslaget er kommentert særskilt, verken i utredningen eller i høringsnotatet, og setter følgelig spørsmålstegn ved om ikke forslaget burde ha vært utredet grundigere.

10.6. Merknader til de enkelte bestemmelser – moderat forslag

Konsesjonsplikt for behandling av særskilte personopplysninger angitt i forskrift – forslagets § 33

Også dette endringsforslaget innebærer at hovedregelen om konsesjonsplikt ved behandling av sensitive personopplysninger oppheves. I stedet skisseres en løsning som legger opp til at det kreves konsesjon *"for å behandle slike personopplysninger som er omfattet av personopplysningsforskriften kapittel [xx]"*.

Det fremgår med andre ord at konsesjonsplikten skal utløses av egenskaper ved personopplysningene, slik som dagens ordning legger opp til. Spørsmålet som melder seg blir igjen hvilke kategorier av personopplysninger som skal underlegges konsesjonsplikten, om ikke nettopp de sensitive, eventuelt i tillegg til spesifikt angitte kategorier, som for eksempel behandles i stor utstrekning i visse bransjer. Det kan for øvrig vises til det som er sagt i forbindelse med det radikale forslaget, og dessuten til Datatilsynets alternative forslag nedenfor.

10.7. Alternativt forslag – konsesjonsplikt med dispensasjonsadgang

Et alternativ som utrederne ikke har vurdert, er å bevare hovedregelen om konsesjonsplikt, supplert med en adgang for Datatilsynet til å gi dispensasjon fra konsesjonsplikten på skjønnsmessig grunnlag. Loven inneholder ingen slik regel i dag. Nettopp dette er årsaken til at enkelte behandlingsformer gjøres til gjenstand for forhåndskontroll, til tross for at det er lite hensiktsmessig. Datatilsynet mener at en slik løsning vil kunne ivareta alle de relevante interesser på en forsvarlig måte, og foreslår herved at en slik regel innføres.

Lovgiver bør utstyre lovteksten med standarder eller kriterier som gir nærmere anvisning på hva tilsynet kan legge vekt på i den forbindelse. Tilsynet antar at det vil være formålstjenlig med nokså skjønnsmessige formuleringer, som for eksempel *"dersom åpenbare grunner gjør det unødvendig med konsesjonsbehandling"*.

Under dagens regime er det altså ikke mulig for Datatilsynet å unnta bestemte behandlinger av personopplysninger fra konsesjonsplikten. Dette medfører at visse behandlinger er underlagt konsesjonsplikt, uten at dette er fornuftig eller ønskelig sett fra noe ståsted. Under en modell som den ovenfor skisserte, kan man beholde koblingen mellom konsesjonsplikt og behandling av *sensitive opplysninger*, mens enkelte konkrete områder trolig bør angis positivt i tillegg. Som eksempler kan nevnes de bransjer som er underlagt konsesjonsplikt gjennom særskilt bestemmelse i forskrift, det vil si bank-, forsikrings-, kredittopplysnings- og telekommunikasjonsbransjen.

Datatilsynet bevarer på denne måten sin mulighet til å utøve en viss forhåndskontroll, i saker av stor personvernmessig betydning – det vil si der vektige personverninteresser står på spill – samtidig som saker som ikke representerer noen reell fare for personvernet unntas konsesjonsbehandling.

Det avgjørende for Datatilsynet er at de registrertes rettigheter ikke blir skadelidende. Dersom konsesjonsinstituttet innskrenkes, må det iverksettes andre kompenserende tiltak, enten i form av økt etterkontroll eller innføring av nye materielle plikter, hvor en utbygget meldeordning kunne inngå som et element – se imidlertid vår reservasjon over. Slike omfattende regelverksendringer bør imidlertid ikke iverksettes utelukkende for endringens skyld – det bør således, med en viss sannsynlighet, kunne konstateres at det finnes fordeler forbundet med endringene, som veier opp for de ulemper som et nytt regelverk vil kunne ha for den registrerte, den behandlingsansvarlige og rettsanvenderen.

10.8. Særskilt om meldeplikten

På bakgrunn av tilsynets alternative forslag, kan reglene om meldeplikt beholdes uendret. De eksisterende problemer med manglende oppfølgning/utbygging av meldeinstituttet kan løses gjennom en endring i praktiseringen av de eksisterende regler.

Vedlegg: Personverndirektivets artikkel 18 og 19:

Artikel 18

Anmeldelsespligt over for tilsynsmyndigheden

1. Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige eller dennes eventuelle repræsentant forud for iværksættelsen af en behandling, der helt eller delvis udføres ved brug af elektronisk databehandling, eller en række sådanne behandlinger, hvis formål er identiske eller indbyrdes relaterede, skal foretage anmeldelse til den i artikel 28 omhandlede tilsynsmyndighed.

2. Medlemsstaterne må kun give mulighed for forenklet anmeldelse eller fritagelse for anmeldelse i følgende tilfælde og på følgende betingelser:

- medlemsstaterne anfører for de typer behandling, hvor det i betragtning af de behandlede oplysninger ikke er sandsynligt, at de registreredes rettigheder eller frihedsrettigheder krænkes, behandlingens formål, hvilke oplysninger eller typer oplysninger der behandles, hvilke registrerede eller kategorier af registrerede der er tale om, til hvilke modtagere eller kategorier af modtagere oplysningerne videregives, samt hvor længe oplysningerne opbevares, og/eller

- de registeransvarlige udpeger i overensstemmelse med den nationale lovgivning, som de er underlagt, en person med ansvar for beskyttelse af personoplysninger, som bl.a. har til opgave

- i fuld uafhængighed at sikre den interne anvendelse af de nationale bestemmelser, der er truffet i medfør af direktivet

- at føre et register over de behandlinger, der gennemføres af den registeransvarlige, og som omfatter de i artikel 21, stk. 2, omhandlede oplysninger

for på denne måde at sikre, at det er ikke sandsynligt, at de registreredes rettigheder og frihedsrettigheder vil kunne krænkes som følge af behandlingen.

3. Medlemsstaterne kan fastsætte, at stk. 1 ikke finder anvendelse på behandlinger, hvis eneste formål er at føre et register, der ifølge love eller administrative bestemmelser er beregnet til at informere offentligheden, og som er tilgængeligt for offentligheden generelt eller for personer, der kan godtgøre at have en legitim interesse heri.

4. Medlemsstaterne kan fritage de behandlinger, der er omhandlet i artikel 8, stk. 2, litra d), for anmeldelsespligt eller fastsætte en forenklet anmeldelse.

5. Medlemsstaterne kan bestemme, at ikke-elektroniske behandlinger af personoplysninger eller nogle af disse behandlinger skal anmeldes, eller foreskrive forenklet anmeldelse af sådanne behandlinger.

Artikel 19

Anmeldelsens indhold

1. Medlemsstaterne præciserer, hvilke oplysninger anmeldelsen skal indeholde. Anmeldelsen skal mindst indeholde følgende oplysninger:

a) navn og adresse på den registeransvarlige og dennes eventuelle repræsentant

b) behandlingens formål

c) en beskrivelse af kategorien eller kategorierne af registrerede og af de oplysninger eller typer af oplysninger, der vedrører dem

d) de modtagere eller kategorier af modtagere, som oplysningerne kan videregives

e) påtænkte overførsler af oplysninger til tredjelande

f) en generel beskrivelse, der giver mulighed for foreløbigt at vurdere, om foranstaltningerne med henblik på behandlingssikkerheden i henhold til artikel 17 er passende.

2. Medlemsstaterne præciserer, efter hvilke procedurer ændringer i de i stk. 1 omhandlede oplysninger skal anmeldes til tilsynsmyndigheden.

11. Fjernsynsovervåking

Omfanget av bruken av kameraovervåkning ser ut til å være økende og kameraovervåkning utgjør en større inngripen i personvernet nå, enn da loven ble vedtatt. Lovrevisjonen bør ha som mål å demme opp for en videre negativ utvikling.

Det bør derfor utformes et regelverk som innebærer en moderat innstramning. Det vil si at regelverket i noe større grad legger føringer for hvilke formål kameraovervåking kan benyttes til, samt sikrer at problemet av en viss alvorlighetsgrad, for at kameraovervåking skal kunne nyttes som et virkemiddel.

Videre bør regelverket legge opp til at de valg som treffes ved iverksetting av kameraovervåking, og også den senere drift, i størst mulig grad reduserer personvernulempene ved overvåkingen.

Disse anliggendene vil bli nærmere kommentert i det følgende.

I Datatilsynets rapport om kameraovervåking fra 2005 og Datatilsynets brev av 19. mai 2009 med supplerende kommentarer, se vedlegg 2 og 3, presenteres sentrale temaer for lovervisjonen, og også Datatilsynets syn på hva som kan eller bør gjøres på dette feltet. Det vil være unaturlig å gjenta store deler av innholdet i rapporten. Det bes derfor om at Datatilsynets høringssvar leses i lys av disse vedleggene.

Det understrekes at det i den nevnte rapportens side 37-40 ikke ble lagt frem et sammenfattende forslag til lovendringer, slik det opplyses i høringsnotatets side 53[32]. De aktuelle sidene er ikke forslag til endringer, men en gjengivelse av lovteksten.

Datatilsynet ser det som utilrådelig å fjerne en særregulering av kameraovervåking slik at denne behandlingsformen utelukkende skal følge lovens alminnelige bestemmelser. Basert på Datatilsynets erfaring er det også grunn til å understreke at særlig på dette området bør hensynet til tilgjengelighet veie tungt ved utformingen av regelverket. Et regelverk som er lett å forstå vil i seg selv være personvernfremmende.

Datatilsynet mener det er naturlig å ta utgangspunkt i dagens løsning, særregulering i et eget kapittel i personopplysningsloven. Datatilsynet ser det videre som tilrådelig at utdypende bestemmelser gis i forskrift og at det i så måte er behov for en gjennomgang av hvilke regler som bør plasseres hvor. Deler av dagens forskriftsbestemmelser bør flyttes til loven. Et eksempel er hovedregelen for sletting av opptak i personopplysningsforskriftens § 8-4. Et annet eksempel kan være rett til innsyn etter forskriftens § 8-5.

[32] Høringsnotatet side 53, andre avsnitt: "Et sammenfattende forslag til lovendringer med kommentarer er inntatt i rapportens side 37-40."

11.1. Om begrepet "fjernsynsovervåking"

Datatilsynet anbefaler at man i lov og forskrift går bort fra begrepet "fjernsynsovervåking" og erstatter det med "kameraovervåking". "Kameraovervåking" benyttes i dagligtalen og vil være dekkende for hva som omfattes av legaldefinisjonen i dag. Begrepet leder tanken i retning av fellesnevneren for innsamlingsmetoden, ulike løsninger som benytter kamera, og ikke fremvisningsmåten.

11.1.1. Definisjonen

Datatilsynet har ingen vesentlige innvendinger mot dagens definisjon. Det bemerkes imidlertid at på det på et område kunne vært behov for en presisering. I dag selges en stadig større andel av kameraovervåkingsløsninger med en innebygd mulighet for lydoverføring/lydopptak. Samtidig er definisjonen i § 36 kun knyttet til billedbehandlingen. Det kan stilles spørsmål ved om dette fremstår tilstrekkelig klart av definisjonen. Én løsning kan være å positivt angi at lydopptak eller lyd som overføres faller utenfor definisjonen. Opptak må vurderes etter lovens alminnelige bestemmelser. Videre bør uttrykket "fjernsynskamera" erstattet med "overvåkingskamera", særlig dersom begrepet "fjernsynsovervåking" byttes ut. Det mest synlige elementet i de fleste overvåkingsanlegg er det publikum kjenner som overvåkingskameraer, ikke fjernsynskameraer og således bringes ordlyden i samsvar med en utbredt og innarbeidet begrepsbruk. Alternativt kan "kamera" benyttes.

I tillegg til spørsmål knyttet til lyd bør det også sees hen til avansert billedbehandling/billedanalyse ved en eventuell utarbeidelse av ny definisjon. Eksempler på slik behandling er ansiktsgjenkjenning, nummergjenkjenning eller kobling av overvåkingsbilder og innslag på kassaapparat. I slike tilfeller skjer det en kobling av informasjon fra overvåkingskameraene og annen "utenforliggende" informasjon (eksempelvis en billeddatabase over etterlyste personer). Det bør tas stilling til om slik billedbehandling (helt eller delvis) bør falle innenfor eller utenfor særreguleringen. Når det gjelder departementets foreløpige merknader i punkt 7.3.2.3 understrekes det at Datatilsynet ikke er av den oppfatning at mobile eller håndholdte kameraer skal omfattes av reglene om kameraovervåkning.

11.2. Behandlingsgrunnlag for fjernsynsovervåking

Datatilsynet støtter innholdet i departementets forløpige merknader i 7.4.2.1. Det er et behov for klargjøring/utdypning av de aktuelle behandlingsgrunnlag for kameraovervåking. Tilsynet stiller seg også positivt til å knytte vurderingen av hva som er en berettiget interesse etter lovens § 8 bokstav f opp mot hvilke formål kameraovervåkingen skal ivareta. Det sees som en styrke at det angis konkrete formål, eksempelvis "liv og helse". Tilsynet mener at denne type formuleringer er med på å peke ut en retning for hva kameraovervåking skal kunne brukes til.

I dag utgjør kostnadene ved å igangsette kameraovervåking ikke lenger en terskel av betydning. Videre er det en utbredt forestilling om at kameraovervåking er et effektivt virkemiddel for å løse en lang rekke problemer. Dette setter personvernet under et betydelig

press. Regelverket bør påpeke at det må ligge tilstrekkelig tungtveiende formål til grunn for overvåkingen, samt hvilke hensyn som anses som aktverdige.

Datatilsynet anbefaler at det innføres en bestemmelse i kapittelet om kameraovervåkning som skjerper de vilkårene som allerede følger av lovens § 8 f på dette område. Tilsynet foreslår at man på lik linje med § 12 som regulerer bruk av fødselsnummer, innfører et tilleggsvilkår som hever terskelen for når denne særskilte formen for behandling av personopplysninger kan benyttes. En slik bestemmelse bør inneholde en utdyping av omstendigheter som må være til stede for at vilkåret i § 8 f skal være oppfylt.

Videre har det på dette området vist seg at skillet mellom ordinære og sensitive personopplysninger, samt kravet om et behandlingsgrunnlag etter lovens § 9, byr på store utfordringer i praksis. Vanskelighetene oppstår særlig når samtykke ikke kan tjene som behandlingsgrunnlag, men en interesseavveining tilsier at overvåking burde være tillatt. Etter Datatilsynets vurdering vil den avveining som skal gjøres etter § 8 f være en god måte å møte også de situasjoner hvor innsamlede opplysninger er følsomme. Om det vedtas en skjerping av kravene som følger av § 8 f, vil en slik bestemmelse kunne være ytterligere egnet til å avklare om det foreligger et gyldig behandlingsgrunnlag i de sammenhenger hvor kameraene er plassert på områder der de i stor utstrekning vil fange opp opplysninger av sensitiv karakter. Tilsynet anbefaler derfor at skillet mellom sensitive og alminnelige personopplyninger oppheves på dette området.

11.2.1. Fjernsynsovervåking på sted hvor en begrenset krets av personer ferdes jevnlig

Datatilsynet slutter seg til departementets forslag om at overskriften til § 38 bør endres i tråd med paragrafens innhold. Videre bør bestemmelsen gis et innhold som bidrar til å klargjøre et skjerpet krav til formålet og som setter den behandlingsansvarlige i stand til å treffe riktige beslutninger. Spesifisering av kravet til behandlingsgrunnlag etter § 8 f og innholdet i § 38 bør i sum sette effektive grenser for utbredelsen av kameraovervåking. Kameraovervåking bør ikke være et "universalmiddel" som legitimt kan brukes til alt fra å redde liv til å unngå forsøpling. Det er viktig at regelverket åpner for at kameraovervåking kan benyttes der dette er nødvendig ut fra tungveiende formål og samtidig verner mot en utstrakt bruk av overvåking, som potensielt bidrar til en ytterligere normalisering av fenomenet. Utfordringen ligger i å finne en rimelig balanse, og et regelverk som klarest mulig evner å formidle grensedragningen til beslutningstakere som i stor grad må ta valget selv – uten noe konsesjonsbehandling eller forhåndsgodkjenning fra Datatilsynet. Regelverket bør i større grad medvirke til nøkternhet i bruk av overvåking ved hjelp av kameraer.

11.3. Varsel om fjernsynsovervåking

Det vises til behandlingen av temaene varsling og informasjon i tilsynets rapport og supplerende brev.

I Datatilsynets tilleggskommentarer i brev fra 2009 tas det til orde for en endring av dagens § 40. Tilsynet ser behov for en bestemmelse som stiller to krav, et minstekrav til varsling gjennom skilter – informasjon som skal nå alle berørte. I tillegg bør det være et krav om ytterligere informasjon etter mønster av personopplysningslovens § 19 til særlig berørte grupper, så langt dette med rimelighet lar seg gjøre. Det sistnevnte kravet kan knyttes til personopplysningslovens § 38 og formuleringen "begrenset krets". Normalt vil det være denne kretsen som har behov for utfyllende informasjon. Så lenge den behandlingsansvarlige kjenner hvem som inngår i den begrensede kretsen er det rimelig å kreve at mer informasjon formidles enn det som skal trykkes på skilter. Eksempelvis bør en arbeidsgiver informere sine ansatte og et borettslag bør gi supplerende informasjon til beboerne.

Datatilsynet anmoder om at spørsmål rundt lovligheten av såkalte "dummy-kameraer" og villedende informasjon i varsel om fjernsynsovervåking blir nærmere behandlet. Datatilsynet ser eksempler på at aktører strekker seg langt for å gi et inntrykk av en reel overvåking, sågar sender inn melding til Datatilsynet. Dummykameraer utgjør ingen behandling av personopplysninger, men strider mot prinsippet om at individer skal få sannferdig og dekkende informasjon om behandling av personopplysninger om dem selv.

Det er i seg selv beklagelig at man forledes til å tro at man er overvåket. Selv om overvåkingen ikke er reell, vil følelsen av å bli overvåket være ekte. At borgerne opplever å bli villedet vil dessuten bidra til å rive ned tilliten til den informasjonen som gis.

Datatilsynet ber departementet vurdere om det kan oppstilles et eksplisitt forbud mot villedende informasjon eller installasjoner, selv om det erkjennes at det vil by på lovtekniske utfordringer å forby "dummy-kameraer", all den tid loven ikke regulerer slike. Etter tilsynets vurdering vil et eventuelt forbud kunne supplere bestemmelsene om informasjonsplikten i kapittelet om kameraovervåkning.

11.4. Øvrige merknader

Datatilsynet stiller seg i utgangspunktet positivt til et opphør av skillet i § 37 første og annet ledd. I rapporten fra 2005 er denne bestemmelsen behandlet. I denne sammenheng vil tilsynet peke på følgende:

Datatilsynet har tatt til orde for at et eget kapittel om kameraovervåking i noe større grad enn i dag har bestemmelser som er særlig tilpasset denne formen for behandling av personopplysninger, men det vil fortsatt være behov for å angi hvilke av de øvrige generelle bestemmelser som også kommer til anvendelse. Etter tilsynets vurdering bør sikkerhetsbestemmelsene i §§ 13, 14 og 15, med tilhørende forskriftsbestemmelser, gjelde for all kameraovervåking. I dag er kun § 13 gitt anvendelse på håndtering av opptak fra

overvåkningskameraer, jf personopplysningsforskriftens § 8-4. Eventuell særregulering bør gjøres gjennom forskriftens bestemmelser for henholdsvis informasjonssikkerhet og internkontroll.

Videre anbefales det at reguleringen av meldeplikt og konsesjonsplikt forenkles. Etter Datatilsynets vurdering bør kameraovervåkning kun være meldepliktig. I tillegg bør Datatilsynet kunne beslutte at en behandling likevel er konsesjonspliktig, etter modell av dagens § 33 annet ledd.

Datatilsynet har erfart at gjeldende regelverk ikke er egnet til å være et effektivt hinder for at privatpersoner overvåker øvrige privatpersoners hus og eiendom. Det er grunn til å tro at den formen for kameraovervåkning har blitt noe mer utbredt de senere år, og det kan ikke være tvil om at slik overvåkning oppleves som meget belastende for de som utsettes for det. Datatilsynets ressurssituasjon begrenser tilsynets mulighet til å følge opp slike saker. Henvendelser fra personer som opplever å bli overvåket av sine naboer resulterer normalt i at påstand blir stående mot påstand, og det er vanskelig for tilsynet å kunne verifisere den enkeltes påstander. Datatilsynet har vurdert det som for ressursskrevende, og heller ikke ønskelig, at tilsynet skal reise landet rundt, å trenge seg inn i private hjem for å gjennomføre stedlige tilsyn for å klarlegge faktum.

De bestemmelser i straffeloven som kunne vært relevante, gir normalt heller ikke politiet noen mulighet til å slå ned på slik overvåking. For at straffelovens § 266 som forbyr hensynsløs adferd skal komme til anvendelse er det et vilkår at adferden, i dette tilfellet overvåkningen, har *til hensikt* å oppfattes som plagsom. § 267 som skal beskytte privatlivets fred, vil kun gjelde krenkelser *"gjennom offentlig meddelelse"*. Det er således et vilkår etter den bestemmelsen at billedmaterialet blir offentliggjort.

Etter personopplysningsloven er det bare brudd på varslingsplikten etter § 40 som er gjort straffbart, ikke overvåkningen i seg selv. Datatilsynet ber derfor departementet vurdere å innføre en ny bestemmelse i straffeloven som eksplisitt forbyr overvåkning av andres private eiendom.

12. Mindreåriges personvern

Departementet ber om høringsinstansenes syn på behovet for et styrket vern av mindreåriges personvern, og hvorvidt dette behovet kan løses gjennom særregulering om beskyttelse av barns personopplysninger.

Dagens personopplysningslov inneholder ikke en særlig regulering av mindreåriges personvern. Datatilsynet har sett eksempler på at dette har fått uheldige konsekvenser, og støtter departementets vurdering av behovet for en endring i loven.

I Barneombudets supplerende rapport til FNs komité for barns rettigheter 2009, har ombudet uttrykt bekymring for at dagens lovgivning ikke i tilstrekkelig grad sørger for vern av barns privatliv. Ombudet påpeker at dagens regelverk forutsetter at foreldre tar gode valg for sine barn, og at det ikke tas høyde for at barn kan ha behov for vern mot foreldres eksponering av

sine barn. Dette gjelder for eksempel i tilfeller hvor foreldre legger ut sensitiv informasjon i barnefordelings- og barnevernssaker på Internett, uten at informasjonen er tilstrekkelig anonymisert. Barneombudet har bedt komiteen om å anbefale Norge å ta nødvendige skritt for å sikre barn et godt rettslig vern av deres privatliv.

Departementet viser i høringsbrevet til straffelovens bestemmelser, som antas å ikke komme til anvendelse i disse tilfellene. Datatilsynet anser dette som en betydelig svakhet ved beskyttelsen av barns rett til personvern, og finner at den foreslåtte endringen av straffelovens § 267 er høyst nødvendig for å sikre barn en reell beskyttelse mot den type overgrep.

I utredernes radikale forslag er det inntatt en ny bestemmelse § 6a, Barns adgang til å opptre som registrert person. Datatilsynet støtter forslaget. Det er forslått at samtykkekompetansen skal avhenge av barnets alder. Ved utformingen av bestemmelsen bør det sees hen til generelle bestemmelser i annen lovgivning om barns samtykkekompetanse, se nedenfor.

Etter tilsynets vurdering bør bestemmelsens overskrift "Barns adgang til å opptre som registrert person" forenkles og endres til for eksempel "Barns rettigheter etter loven", og med en henvisning til hvilke bestemmelser som er relevante. Forståelsen av den foreslåtte overskriften forutsetter kunnskap om definisjonene i loven, og Datatilsynet mener at innholdet blir mer tilgjengelig dersom man forenkler ordlyden.

12.1. Vedrørende mindreåriges samtykkekompetanse

Datatilsynet vurderer det som positivt at det foreslås å innta en bestemmelse om barns samtykkekompetanse i personopplysningsloven. Tilsynet mener at samtykkekompetansen må samsvare med barnelovens og barnekonvensjonens system, hvor barnet gis gradvis større selvbestemmelsesrett på bekostning av foreldrenes samtykkekompetanse.

Utgangspunktet i personopplysningsloven, er at foreldre har samtykkekompetanse til behandling av personopplysninger på vegne av sine barn, jf Ot.prp. nr. 92 (1998-99)s. 103. Datatilsynet har i sin praksis vurdert mindreåriges samtykkekompetanse i den enkelte sak. Barnets alder og modenhet har blitt vurdert i forhold til behandlingens formål, art og omfang samt opplysningenes innhold.

Datatilsynets og Forbrukerombudets veileder "Barn og unges personopplysninger" redegjør for hvilke spesielle hensyn næringsdrivende bør ta når de innhenter og behandler personopplysninger om barn og unge i forbindelse med markedsføring. Departementet har vurdert hvorvidt retningslinjene skal kodifiseres. Datatilsynet støtter et lovforslag som samsvarer med barnelovens generelle system, og som ikke baseres på retningslinjer med et begrenset anvendelsesområde.

Utgangspunktet om foreldres samtykkekompetanse følger også av barnelovens bestemmelser. Foreldrenes kompetanse er imidlertid begrenset av barnets egen kompetanse til å samtykke og deres rett til å bli hørt, jf barnelovens §§ 31 - 33 og barnekonvensjonens artikkel 12.

I den foreslåtte § 6 a om barns rettigheter deles mindreårige inn i tre alderskategorier; fra 7-12 år, fra 12-15 år og fra 15-18 år. Dette samsvarer med tilsvarende regulering i barneloven med

unntak av for den yngste gruppen. For barn fra 7 til 12 år bestemmer barneloven at barnet *skal* få si sin mening i før det tas avgjørelser i forhold som angår dem. Utrederne foreslår imidlertid at foreldrene til barn i denne alderskategorien kan opptre alene, men at de *bør* spørre egne barn om deres mening. Datatilsynet slutter seg til utredernes forsalg. Barn i denne aldersgruppen kan i liten grad anses å ha forutsetninger for å vurdere rekkevidden av et samtykke til behandling av deres personopplysninger.

12.2. Vedrørende bestemmelse om unntak fra innsyn

Det foreslås unntak for mindreåriges rett til innsyn for de tilfellene dette anses utilrådelig. I dagens lov § 23, litra c), kan det gjøres unntak fra innsynsretten der dette anses utilrådelig i visse tilfeller. Datatilsynet slutter seg til et slikt forslag. I vurderingen av hva som er utilrådelig må det tas utgangspunkt i barnets alder og modenhet, og det må legges vekt på hva som er til det beste for barnet.

12.3. Barnets beste - reservasjon

Datatilsynet har i sin praksis sett at det er vanskelig å gripe inn i tilfeller hvor foreldre handler i strid med sine barns rett til privatliv og personvern, selv om det etter dagens regelverk er utvilsomt at foreldres samtykkekompetanse overfor sine barn ikke er ubegrenset.

Som eksempel på en alternativ løsning, vil Datatilsynet trekke fram helseforskningsloven som trådte i kraft 1. juli 2009. §§ 17 og 18 i loven omhandler mindreåriges samtykkekompetanse i forbindelse med deltakelse i forskning. § 17 regulerer grensene for foreldres kompetanse til å samtykke på vegne av sine barn, og denne kompetansen avhenger av og innskrenkes ut i fra barnets alder. I § 18 tredje ledd, har lovgiver inntatt et krav om at det ved et "stedfortredende samtykke" skal foreligge presumert samtykke fra deltakeren:

"For personer uten samtykkekompetanse kreves det at det ikke er grunn til å tro at vedkommende ville motsatt seg deltakelse i forskningsprosjektet hvis vedkommende hadde hatt samtykkekompetanse"

Etter Datatilsynets vurdering er det hensiktsmessig å innta en tilsvarende betingelse i personopplysningsloven, hvor kravet om at barnets beste skal være et grunnleggende hensyn, jf. barnekonvensjonens artikkel 3.

12.4. Generelt om "stedfortredende samtykke"

Datatilsynet vurderer det som hensiktsmessig å innta tilsvarende reservasjon i "stedfortredende samtykke" i andre tilfeller hvor den registrerte selv ikke kan samtykke, f eks overfor umyndiggjorte personer.

13. Personvernombudsordningen

13.1. Forankring av personvernombudsordningen

Personvernombudsordningen bygger på personverndirektivets artikkel 18 nr. 2 jf. artikkel 20 nr. 2 jf. fortalen punkt 49. Der medlemsstatene kan fastsette unntak fra meldeplikten hvor det ikke er sannsynlig at behandlingen av opplysninger vil kunne krenke registrertes rettigheter og friheter. Det oppstilles et vilkår om at personen som har ansvar for opplysningsvernet skal kunne utøve sitt verv i *full uavhengighet.*

Personopplysningsloven inneholder ingen bestemmelser om personvernombud. Det følger av forarbeidene at ordningen ikke er nærmere drøftet av utvalget, og heller ikke har vært i fokus under høringen. Det åpnes for å iverksette frivillige prøveordninger i samarbeid med de behandlingsansvarlige, men "Dersom man i lys av erfaringene med en utprøving av ordningen finner det ønskelig å etablere et mer permanent og generelt system med utpeking av dataansvarlige, vil det kunne være behov for mer konkret å regulere de dataansvarliges oppgaver og ansvar i loven.", jf. Ot.prp. nr. 92 (1998-1999) side 58. Dette er bakgrunnen til at de eneste bestemmelsene som nevner personvernombudsordningen finnes i personopplysningsforskriftens § 7-12 og § 7-27.

Etter personopplysningsforskriftens § 7-12 kan Datatilsynet samtykke i at det gjøres unntak fra meldeplikt, "dersom den behandlingsansvarlige utpeker et *uavhengig* personvernombud som har i oppgave å *sikre* at den behandlingsansvarlige følger personopplysningsloven med forskrift."

Den andre bestemmelsen som nevner personvernombudsordningen er personopplysningsforskriftens § 7-27, hvoretter: "Behandling av personopplysninger i forbindelse med et *forskningsprosjekt* er unntatt fra konsesjonsplikt" dersom prosjektet er tilrådd av personvernombud. Unntaket gjelder ikke forskningsprosjekter av stort omfang og lang varighet, samt forskning på store datasett som ikke er pseudonymisert eller avidentifisert på annen sikker måte.

13.2. Generelle merknader

Dagens ordning er basert på frivillighet. Dette aspektet ved ombudsordningen bør videreføres, men det anbefales at instituttet som sådan forankres i loven, dog slik at det ikke oppstilles detaljkrav i lovteksten. Personvernombudsordningen har vært en prøveordning og den er fortsatt i utvikling, og det er hensiktsmessig med en dynamisk regulering som gjør at ordningen kan utvikle seg over tid.

Tilsynet foreslår at ordningen forankres i lov ved at Datatilsynet pålegges en plikt til å legge til rette for opprettelse av uavhengige personvernombud. En slik oppgave for tilsynet bør inntas som en nytt krav i den eksisterende § 42 tredje ledd.

Om en sertifiseringsordning er ønskelig fra departementets side, gjøres det oppmerksom på at Datatilsynet per dags dato ikke har ressurser til å kunne gjennomføre en reell kontroll av hvordan forholdene ved virksomheten er før "sertifikat" utstedes. Tilsynet er følgelig negativ

til en slik sertifiseringsordning, da den vil gi skinn av å være en kvalitetssikring av virksomheten, uten at det foreligger noen forutgående kontroll som sikrer en etterlevelse av kravet som berettiger en slik sertifisering.

13.3. Begrepet "personvernombud"

Datatilsynet mener det vil være fordelaktig å bevare begrepet personvernombud. Det pekes særlig på at det er lagt inn ressurser på å markedsføre ordningen, samt gi den et innhold som skaper positive konnotasjoner til rollen som personvernombud. Datatilsynet ser imidlertid at begrepet "ombud" rent språklig synes å vise til at personen som utpekes av virksomheten skal ha en funksjon som ikke vil være dekkende for dagens ordning. Dette vil imidlertid også kunne gjøre seg gjeldende for begreper som personvernansvarlig, personvernrådgiver og personopplysningsrådgiver. Det vises særlig til at personen ikke kan være *ansvarlig* for behandlingen av personopplysninger når ansvaret etter loven påligger den behandlingsansvarlige. Datatilsynet tror videre at det vil kunne være vanskelig å selge inn en ordning som profileres med betegnelser som personvernrådgiver eller personopplysningsrådgiver. Det er ikke til å komme utenom at merkevarebyggingen av begrepet vil være av betydning, og da Datatilsynet er av den oppfatning at det ikke bør gjøres særlige unntak fra øvrige krav i loven, jf. merknader under, vil begrepet og profileringen av virksomheter med særlig personvernfokus være av sentral betydning. Dersom departementet skulle være av en annen oppfatning, vil Datatilsynet foretrekke begrepet personvernrådgiver, jf. over.

13.4. Eksterne personvernombud

Per dags dato foreligger det ingen krav knyttet til personvernombudets tilknytning til virksomheten, noe som innebærer at også eksterne personvernombud kan benyttes. Heller ikke personverndirektivet gir noen anvisning på dette punktet, foruten å oppstille et krav om at personen som oppnevnes må være uavhengig i sin stilling. Et tilsvarende krav oppstilles i personopplysningsforskriftens § 7-12.

Det følger av departementets høringsnotat at ombudenes primære oppgave som utgangspunkt bør være å bidra til at behandlingsansvarlige etterlever personvernlovgivningen. Videre fremgår det at: "I tillegg bør ombudet i størst mulig utstrekning kunne bistå registrerte personer, ansatte og ledelsen hos den behandlingsansvarlige. Dette tilsier at personvernombudet bør være en person som naturlig tar del i, eller idet minste har inngående kjennskap til den behandlingen av personopplysninger som foregår." På den annen side vil en fjerning av adgangen til å benytte eksterne ombud kunne medføre at en rekke virksomheter vil avskaffe ordningen. Dette vil i særlig grad gjelde virksomheter som er knyttet opp mot Norsk Samfunnsvitenskapelig Datatjeneste (NSD).

Datatilsynet ser fordeler og ulemper ved begge løsninger, og er langt på vei enig i de innsigelser som er kommet i forhold til både en intern og en ekstern ordning. Tilsynet har sett eksempler på at begge løsninger kan være gode i praksis, men også det motsatte. Hvordan organiseringen fungerer i praksis vil imidlertid være nært knyttet opp mot hvilke krav som

stilles til ombudet, og hvilke oppgaver ombudet skal ha, mer enn den formelle tilknytningen til virksomheten.

13.5. Personvernombudets oppgaver

Personvernombudsordningen er lite synlig i dagens regelverk, noe som etter Datatilsynets vurdering er uheldig. Ved å innta en bestemmelse om ordningen i personopplysningsloven vil hjemmelsgrunnlaget for ordningen klarlegges, noe som er av avgjørende betydning dersom man skal tillegge ombudet rettslige plikter av et visst omfang. Videre vil ordningen synliggjøres.

Datatilsynet er imidlertid av den oppfatning at en detaljregulering av innholdet i ordningen bør unngås, jf. over.

Tilsynet vil poengtere viktigheten av å ta stilling til hva slags funksjon et ombud skal inneha før man kan vurdere nærmere hvilke oppgaver, plikter og rettigheter en virksomhet med ombud skal ha. Avgjørende vil i så måte være om ombudet skal fungere som en utstrakt arm for Datatilsynet, eller om ombudet primært skal fungere som en ressursperson i virksomheten. Det presiseres i forlengelsen av dette at det er den behandlingsansvarlige som har det rettslige ansvaret for en behandling av personopplysninger etter personopplysningsloven. Man bør følgelig utvise forsiktighet med å pålegge individuelle plikter for et personvernombud.

Ettersom personvernombudsordningen fremheves som frivillig, og da Datatilsynet ikke har noen reell mulighet til å overprøve hvorvidt et oppnevnt ombud rent faktisk har en uavhengig stilling, bør rollen som ombud i hovedsak sentreres om det å fungere som en ressursperson i virksomheten. Etter Datatilsynets vurdering bør således fokus ligge på at personvernombudet skal bistå/rådføres i personvernspørsmål, men ikke pålegges konkrete plikter i lovs form knyttet til oppfølging av enkeltsaker, utforming av personvernpolicyer eller å skrive årsmeldinger, jf. Schartum/Bygrave side 138. Tilsynet vil følgelig fraråde å lovhjemle forslag til ny § 27b.

13.6. Personvernombudets uavhengighet

Som nevnt innledningsvis oppstiller personverndirektivet og personopplysningsforskriften et krav om uavhengighet for personvernombudet. Kravet må være oppfylt for å kunne gjøre unntak fra meldeplikten eller øvrige lempninger.

Tilsynet vil starte med å fremheve viktigheten av at den behandlingsansvarlige legger til rette for at personvernombudet kan inneha en uavhengig rolle som ombud, samt gis adgang til å delta på prosesser som har betydning for personvernet. En slik tilrettelegging er av avgjørende betydning for at ordningen skal fungere, og for at personvernombudet skal kunne ivareta de interessene som det er satt til å verne.

Datatilsynet stiller imidlertid spørsmålstegn ved hvorvidt et personvernombud som utpekes av den behandlingsansvarlige på bakgrunn av en frivillig ordning, i realiteten kan regnes som uavhengig. Videre kan Datatilsynet vanskelig kontrollere om vilkåret er oppfylt i praksis. I

forlengelsen av dette vil Datatilsynet fremheve at det ikke er ønskelig med en ordning hvor personvernombudet skal fungere som tilsynets utstrakte hånd, da dette kan fremstå som problematisk ut i fra et forvaltningsmessig perspektiv. Det er således ikke ønskelig å etablere en ordning hvor Datatilsynet har en styrings- eller instruksjonsmyndighet over ombudet. Dette medfører at man etter Datatilsynets vurdering bør være tilbakeholdne med å gi lettelser i form av unntak fra konsesjonsplikt eller gjøre andre unntak fra regelverket som kan innebære en fare for personvernet. Dette vil kommenteres nærmere i det følgende.

13.7. Lovbestemte fordeler ved opprettelse av personvernombud

Som nevnt over, samt i departementets høringsnotat, er Datatilsynet av den oppfatning at det ikke er behov for lovbestemte fordeler ved opprettelse av personvernombud. Årsakene til at dette fremstår som lite hensiktsmessig er flere. En viktig begrunnelse vil være at personvernombudsordningen etter tilsynets vurdering fortsatt bør være en frivillig ordning som primært har verdi ved at virksomheten får kompetanse og opplæring innenfor personvern, samt kan profilere seg som en virksomhet som er opptatt av personvern. Incentivene for ordningen bør være nettopp å forbedre personvernet i virksomheten, ikke å gjøre rutinene for behandling av personopplysninger dårligere enn per dags dato. Datatilsynet vil i den forbindelse på det sterkeste fraråde en vedtagelse av forslag til ny § 27a, hvoretter Schartum/Bygrave forslår at virksomheter med personvernombud kan fritas fra kravet til internkontroll etter lovens § 14. Formålet med etablering av internkontroll er nettopp å sikre en etterlevelse av personopplysningslovens og personopplysningsforskriftens krav, og er i så måte et viktig verktøy for virksomhetene for å kartlegge behandlingen av personopplysninger og hvordan behandlingen skal gjennomføres i tråd med lovens krav. Et personvernombud kan på ingen måte kunne stille som garantist for at personopplysningslovens bestemmelser med forskrift etterleves. Tvert i mot bør etablering av et internkontrollsystem være et klart vilkår for at en virksomhet skal få godkjenning på en søknad om opprettelse av personvernombud.

Videre legges det opp til at Datatilsynet skal tilby særskilte og kostnadsfrie informasjons-, veilednings- og opplæringstjenester. Datatilsynet er positiv til at kurs og opplæring skal være gratis for virksomheter som velger å benytte seg av ordningen, da tilsynet ser virksomhetenes kompetanse og fokus på personvern som en sentral verdi, som i seg selv bør kunne være med på å markedsføre personvernombudsordningen. En slik plikt vil nødvendigvis medføre økte kostnader for tilsynet, noe som det må tas hensyn til ved utarbeidelsen med regelverket.

13.8. Opphør av personvernombudsordningen

Datatilsynet vil innledningsvis poengtere at etter dagens tolkning av regelverket er en avtale om å etablere personvernombud i en virksomhet, en trepartsavtale mellom den behandlingsansvarlige, det enkelte ombud (som er en fysisk person), og Datatilsynet. Det radikale forslaget fra Schartum/Bygrave synes imidlertid å legge opp til sertifiseringsordning hvor kun den behandlingsansvarlige og Datatilsynet nevnes som pliktsubjekter.

Tilsynet ønsker en videreføring av ordningen hvor rollen som personvernombud er tildelt en fysisk person, og ikke som en sertifisering av virksomheten som sådan. Årsaken til dette er at en sertifiseringsordning eventuelt bør bygge på fastlagte kriterier som må være oppfylt for å

kunne markedsføre seg som en del av personvernombudsordningen. Slike krav vil vanskelig kunne oppstilles på et generelt plan, og vil medføre bruk av store ressurser fra tilsynets side, som det per dags dato ikke finnes kapasitet til å iverksette. En sertifisering uten at det stilles krav, eller hvor det stilles krav som Datatilsynet er i stand til å kontrollere/vurdere, vil gi ordningen et skinn av troverdighet som ikke kan rettferdiggjøres. Datatilsynet er følgelig av den oppfatning at trepartsavtalen fortsatt bør legges til grunn for en etablering av ordningen.

Datatilsynet ser behovet for å kunne ha sanksjoner som kan iverksettes dersom ombudsordningen viser seg å ikke fungere etter sin hensikt i en virksomhet eller organisasjon. Samtidig innser tilsynet at det er uheldig å knytte sanksjoner til personvernombudsordningen ved brudd på personopplysningsloven når ombudsrollen er tildelt en fysisk person. Det enkelte ombud bør ikke pålegges en personlig plikt til å kontrollere at lovens krav oppfylles. Som nevnt tidligere tilligger den overordnede plikten til å ivareta personopplysningslovens krav den behandlingsansvarlige. Det gjøres for ordens skyld oppmerksom på at en tilsvarende sanksjonsbestemmelse ikke finnes i Sverige.

14. Ny bestemmelse om bruk av fødselsnummer og biometri

I rapporten "Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12" fra 2008 uttales det at personvernhensyn taler for å begrense bruken av fødselsnummer til offentlig sektor og utveksling av personopplysninger mellom private og offentlig sektor. Det fremmes ikke et konkret forslag om slik lovendring, fordi det er usikkert hvilke konsekvenser dette vil få for private virksomheter. I rapporten anbefales det at departementet ser nærmere på denne muligheten. Datatilsynet støtter opp under en slik anbefaling. Bruk av entydige identifikatorer er en nødvendighet hos de fleste behandlingsansvarlige. Dette kravet innebærer likevel ikke at den behandlingsansvarlige må bruke fødselsnummer. Utover å være entydig er fødselsnummer som identifikator også statsautorisert og av varig karakter. Betydelig mengder informasjon er knyttet til dette nummeret, hvilket gjør at konsekvensene ved lekkasjer eller tilsiktede ulovlige utleveringer kan bli meget store. Slike unike identifikatorer bør kun brukes der det er helt nødvendig, ikke basert på hva behandlingsansvarlig finner praktisk. Etter tilsynets vurdering bør praksisen rundt bruk av fødselsnummer strammes inn til sitt opprinnelige formål, nemlig å sikre entydighet i forvaltningen.

Når det gjelder forslaget til lovendring er Datatilsynet enig i at det er hensiktsmessig å regulere bruk av fødselsnummer og biometri i hver sin bestemmelse. Bruken av opplysningene reiser forskjelligartede spørsmål. Fødselsnummeret er velegnet til identifikasjon, men uegnet til autentisering, mens fingeravtrykk derimot kan brukes til begge deler.

Dersom man ser bort fra forslagets fjerde ledd om autentisering, synes Datatilsynet i all hovedsak at lovforslaget har mange positive sider ved seg, men ser samtidig at det er rom for enkelte forbedringer som foreslås nedenfor.

14.1. Krav om behovsvurdering

Datatilsynet synes gode grunner taler for at det innføres et vilkår om at den behandlingsansvarlige må ha gjennomført en vurdering, som klart viser at nødvendighetskravet for å bruke fødselsnummer er oppfylt. Dette kravet vil kunne bidra til å redusere noe av feilbruken av fødselsnummer, som blant annet skjer av bekvemmelighetshensyn og mangelfull kunnskap om fødselsnummerets uegnede verdi som legitimasjon. Vurderingen vil også kunne etterspørres av publikum og Datatilsynet i forbindelse med klagesaker og tilsyn. Det er imidlertid uheldig å bruke begrepet risikoanalyse som er godt innarbeidet ved vurderingen av spørsmål vedrørende informasjonssikkerhet, og som viser til noe ganske annet. Datatilsynet foreslår at man i stedet bruker begrepet behovsvurdering. Det bør for øvrig nedfelles et dokumentasjonskrav knyttet til analysen, tilsvarende personopplysningslovens krav til dokumentasjon av risikovurdering og internkontrollrutiner.

14.2. Datatilsynets kompetanse

Datatilsynet foreslår en omformulering av tredje ledd, slik at ikke enhver fare for personforveksling omfattes. Det er kun i de tilfeller hvor konsekvensene av en personforveksling vil få betydelige følger for enkeltpersoner, at Datatilsynet uttrykkelig pålegger bruk av fødselsnummer. Et eksempel på dette er ved kredittsjekk, hvor personforveksling kan medføre at vedkommende for eksempel ikke får innvilget lån.

14.3. Forslagets § 11 fjerde ledd om et forbud mot å bruke fødselsnummer ved autentisering

Datatilsynet vil sterkt fraråde at det inntas en bestemmelse som tillater bruk av fødselsnummer for autentisering sammen med andre opplysninger som ikke er åpent tilgjengelig. Slik Datatilsynet ser det vil fjerde ledd stride mot hovedvilkårene for bruk av fødselsnummer i første ledd. Bruk av fødselsnummer skal være nødvendig for å oppnå sikker identifisering. Som påpekt i forarbeidene[33] vil kravet til nødvendighet *"bare være oppfylt dersom andre og mindre sikre identifikasjonsmidler, som f eks navn, adresse og kundenummer ikke er tilstrekkelig"*. Dette argumentet har fortsatt gyldighet. Fødselsnummer skal ikke brukes ved pålogging, eksempelvis som brukernavn. Dette gjelder i tilknytning til internettjenester så vel som interne datasystemer, for eksempel på en arbeidsplass. Bruk av fødselsnummer i forbindelse med autentisering innebærer at fødselsnummer tillegges en legitimasjonsvirkning det ikke er egnet for. Det er videre uttalt i flere avgjørelser av Personvernnemnda[34] at fødselsnummer er helt uegnet for autentisering.

Å bruke fødselsnummer som brukernavn, passord eller som annet element i påloggingsrutinen er en unødvendig bruk av fødselsnummeret, med betydelige sikkerhetsmessige implikasjoner. Nettjenester som bruker fødselsnummer ved innlogging har vist seg å ha svakheter, noe som gjør behovet for å unngå fødselsnummer ved pålogging enda sterkere. Etter tilsynets

[33] Ot prp 92 (1998-99) side 114
[34] PVN 2006/7, PVN 2006/8, PVN 2006/9, PVN 2006/10 og PVN 2006/11

vurdering bør det derfor innføres et nytt fjerde og femte ledd i den foreslåtte bestemmelsen som eksplisitt forbyr bruk av fødselnummer som legitimasjon og ved pålogging/autentisering. Samtidig åpnes det for et unntak i særskilte tilfeller, hvor det kan søkes om at Datatilsynet gir tillatelse gjennom et enkeltvedtak. Liknende unntak etter vedtak fra Datatilsynet finnes i flere andre bestemmelser i personopplysningsforskriften, blant annet forskriftens § 4-7 vedrørende kredittopplysningsvirksomhet.

14.4. Forslagets § 11 femte ledd om forsendelser som inneholder fødselsnummer

Datatilsynet synes det er hensiktsmessig at bestemmelser som gjelder fødselsnummer er samlet i én felles bestemmelse, og at personopplysningsforskriften § 9-2 derfor overføres til den foreslåtte § 11.

14.5. Erstatningsansvar

I utredningen anbefales det at man innfører et objektivt erstatningsansvar i de tilfeller hvor fødselsnumre på et eller annet vis har kommet på avveie. Datatilsynet anbefaler ikke en slik løsning. Tilsynet er av den oppfatning at de generelle reglene om erstatningsplikt i tilstrekkelig grad beskytter de berørtes interesser. Det antas dessuten at det vil være vanskelig å konstatere årsakssammenheng mellom lekkasjen og et eventuelt økonomisk tap. Videre vil det i mange sammenhenger være mer naturlig å plassere tapet hos den virksomhet, hvis systemer tillater at fødselsnumre lar seg misbruke.

14.6. Saksdokumenter som inneholder fødselsnumre

Datatilsynet anmoder departementet om å vurdere å innføre en særskilt plikt for organer som er underlagt offentlighetsloven til å sladde fødselsnumre fra dokumenter som ikke er unntatt offentlighet. Datatilsynet er ikke kjent med at det eksisterer en slik eksplisitt plikt etter gjeldende regelverk.

14.7. Ny bestemmelse om bruk av biometriske metoder mv.

Datatilsynet ser behovet for at det i bestemmelsen skilles mellom formålene identifisering og autentisering. Videre tilsluttes forslagets uttrykkelige regulering av behandlingsgrunnlag for disse formålene. Etter tilsynets syn er det imidlertid unødvendig å henvise til legaldefinisjonen av samtykke og påpeke at kravet om informasjon til den registrerte skal være i samsvar med innholdet i informasjonsplikten i personopplysningsloven § 19. Det må kunne legges til grunn at de behandlingsansvarlige på dette området gjør seg kjent med legaldefinisjonene.

Den viktigste grunnen til å være varsom med bruk av biometri er at biometriske kjennetegn unikt beskriver det enkelte individ, og er uløselig knyttet til oss. Biometri kan også være bærer av annen informasjon enn det rent identifiserende, eksempelvis DNA. Videre kan biometrisk avlesning av øynene, ansiktet eller benbygningen si noe om helse og etnisk bakgrunn. Hva som ellers kan utledes av slike opplysninger eller avlesninger på sikt er

uoverskuelig. Videre kan innsamling av biometriske opplysninger gjennomføres uten at vi selv er klar over det. Vi legger eksempelvis igjen fingeravtrykk overalt hvor vi ferdes.

Datatilsynet anbefaler derfor at det innføres et vilkår som fanger opp usaklig og unødvendig bruk av biometriske metoder, også når det er innhentet samtykke. Bruk av biometriske kjennetegn bør benyttes med varsomhet og forbeholdes tilfeller hvor det er tungtveiende behov for bekreftelse av påstått identitet. Dette kan løses ved å tilføye et vilkår i forslagets tredje ledd.

Det faktum at det er opplysninger som er uløselig knyttet til oss, tilsier at de skal behandles med ekstra varsomhet. Prinsippet om at man bør velge den løsningen som er minst inngripende for personvernet, samt de nevnte særlige egenskapene ved biometriske kjennetegn, taler for at det oppstilles et vilkår som forhindrer bruk av biometriske kjennetegn av bekvemmelighetshensyn.

Datatilsynet fastholder at det er behov for uttrykkelig regulering i lov om at bruk av biometriske metoder som innebærer behandling av sensitive opplysninger er konsesjonspliktig og at all annen behandling av biometriske opplysninger som faller inn under lovens virkeområde, er meldepliktig. Dette behovet er det redegjort for i brev til Justis- og politidepartementet den 31. mars 2006.

15. Internkontroll og informasjonssikkerhet

Bestemmelsene om internkontroll i § 14, informasjonssikkerhet i § 13 og om databehandleres rådighet over personopplysninger i § 15 står i nær sammenheng med hverandre. Det er derfor etter Datatilsynets vurdering nødvendig å se bestemmelsene i sammenheng. Dessuten bør rekkefølgen på bestemmelsene endres, slik at den mer generelle internkontrollbestemmelsen plasseres foran bestemmelsen om informasjonssikkerhet. En slik rekkefølge vil gjøre det enklere å forstå at informasjonssikkerhet er en del av internkontrollen, og ikke omvendt, slik situasjonen til dels oppfattes i dag.

Direktiv 95/46 EF stiller i avsnitt VIII, artikkel 17 krav til sikkerhet ved behandlingen. Artikkel 17 nr. 1 og 2, gjennomføres ved personopplysningslovens § 13. Nr. 3 og 4 gjennomføres i personopplysningslovens § 15 som omhandler databehandlers rådighet over personopplysninger.

Det stilles krav til planlagte og systematiske tiltak for å sikre generell etterlevelse av lovens krav (internkontroll) og for å sikre tilfredstillende informasjonssikkerhet. For begge kategorier kreves det dokumentasjon som skal være tilgjengelig for medarbeiderne i den behandlingsansvarliges virksomhet og databehandlere, samt for Datatilsynet og Personvernnemnda.

Bestemmelsene om internkontroll og informasjonssikkerhet skal sikre en forsvarlig behandling av personopplysninger. Dette inkluderer å identifisere plikter, gjøre overordnede valg, legge til rette for forsvarlig behandling, samt å følge opp at kravene etterleves i organisasjonen. Datatilsynet har gjennom tilsyn og saksbehandling kunne konstatere at dette

målet ikke oppnås i tilstrekkelig grad. Hovedgrunnene til det er en blanding av manglende kjennskap til eller forståelse av regelverket, samt manglende motivasjon. Etterlevelse av regelverket vil kreve ressurser og i mange tilfeller stå i en prioriteringskonflikt med virksomhetens kjerneoppgaver.

Spesielt for mindre virksomheter fremstår regelverket som tungt. Dette kan delvis forklares med at regelverkets bestemmelser er generelle og derfor krever en egeninnsats og konkrete vurderinger for å kunne etterleves. Små virksomheter har et behov for å få skreddersydde løsningsforslag som de kan arbeide videre med i egen organisasjon.

Dagens lovregulering bygger på en grunnpilar – *planlagte systematiske tiltak*. Datatilsynet betrakter disse premissene som fornuftige og hensiktsmessige å videreføre. Planlagte og systematiske tiltak er velforankrete og tidsuavhengige, samtidig som de angis som anerkjente virkemidler i annet regelverk den behandlingsansvarlige må forholde seg til.

15.1. Internkontroll § 14

Bestemmelsene om internkontroll skal sikre en forsvarlig behandling av personopplysninger i virksomhetene. Dette inkluderer å identifisere plikter, gjøre overordnede valg, legge til rette for forsvarlig behandling av personopplysninger samt å følge opp at dette etterleves i organisasjonen. Grunntanken er forestillingen om at pliktsubjektet gjennom en systematisk tilnærming vil ha en bedre mulighet til å etterleve regelverket. Kravene til internkontroll skal tjene som en garantist for at øvrige krav i personopplysningsloven følges, og § 14 er således en av de mest sentrale bestemmelsene i loven. Internkontroll er derfor så godt som alltid tema under Datatilsynets tilsyn.

Datatilsynets kontroller viser imidlertid at svært mange virksomheter har til dels store mangler i internkontrollsystemet. Slik Datatilsynet oppfatter det er årsaken til dette at virksomhetene enten ikke kjenner til regelverket på dette området, eller at de ikke forstår hva kravet til internkontroll innebærer og som allerede påpekt, manglende motivasjon. Regelverket som sådan vurderes imidlertid som hensiktsmessig av virksomheter som har en viss innsikt i tematikken, selv om det nok ofte kan oppfattes som noe omstendelig for mindre virksomheter som kun behandler relativt trivielle personopplysninger.

Datatilsynets erfaringer støttes av Personvernundersøkelsen fra 2005 som er nevnt innledningsvis i høringsbrevet. Ulike offentlige og private virksomheter ble her blant annet spurt om deres kunnskaper og holdninger til personvern og til personvernregelverket. Om lag halvparten av de spurte virksomhetene sa at de hadde etablert et internkontrollsystem som dokumenterte rutiner og tiltak for å sikre at behandlingen av personopplysninger skulle skje i tråd med kravene i personopplysningsloven. Kontrollspørsmål viste imidlertid at langt færre kunne bekrefte at de hadde gjennomført tiltak som burde vært en del av en slik internkontroll. I samme undersøkelse svarte 74 % at de trodde at mangel på kunnskap om lovgivningen var den viktigste årsaken til at regelverket ikke ble fulgt.

Regelverket om internkontroll er i dag utdypet i personopplysningsforskriftens kapittel 3. Datatilsynet har sett på hvordan forskriften kan bedres for å tilgjengeliggjøre innholdet. Etter

vår vurdering er imidlertid ikke dette tilstrekkelig. Datatilsynet støtter Schartum og Bygrave i deres vurdering av at sentrale krav bør fremkomme av loven. Sentrale krav bør formidles på en slik måte at pliktsubjektene umiddelbart forstår at de har en handlingsplikt. Kravene bør utdypes i forskrift.

Datatilsynet viser til at brudd på personopplysningsforskriftens kapittel 3 om internkontroll er straffesanksjonert, jf. forskriftens § 9-3. Selv om forskriften står for seg selv er det uheldig at § 14 er såpass vagt formulert at pliktsubjektene ikke oppfordres til å gå videre til kapittel 3 i forskriften.

I tillegg til å endre regleverket vil bedre, og mer tilgjengelig informasjon kunne løse deler av problemet med manglende etterlevelse. Datatilsynet har derfor utarbeidet et veileder med et sett med maler for virksomheter som skal innføre internkontroll. Dette kommer imidlertid som supplement til et enklere regelverk.
Datatilsynet er av den oppfatning av at det bør sees hen til annet lovverk om internkontroll når internkontrollbestemmelsene på personvernområdet skal utformes. Et mer helhetlig internkontrollregelverk vil etter Datatilsynets vurdering gjøre det enklere for virksomheter å forstå og etterkomme internkontrollkravene.

15.1.1. Kommentarer til de foreslåtte endringer

Datatilsynet støtter ikke departementets forslag om at det bør fremkomme av lovteksten at internkontrollen kan deles opp i en styrende, gjennomførende og kontrollerende del. Denne inndelingen er et metodisk virkemiddel som eventuelt bør nedfelles i forskrift, ikke pålegges som en plikt i loven. Datatilsynet er imidlertid enig i at enkelte helt sentrale internkontrollkrav, slik som fastsetting av den behandlingsansvarlige og utarbeidelse av en oversikt over personopplysninger som behandles, med fordel kan fremkomme av loven. Når det gjelder krav til rutiner for konkrete gjennomførende plikter mener imidlertid Datatilsynet at disse bør fremkomme av forskrift og veileder til lov og forskrift. Det vil kunne være behov for å endre slike krav uten at man må gå veien om lovendring, og en opplisting av formelle krav vil lett kunne bli oppfattet som uttømmende.

Datatilsynet mener at en hensiktsmessig utforming av lovens § 14 må sees i sammenheng med endring av personopplysningsforskriftens kapittel 3. Datatilsynet bistår gjerne i utformingen av disse bestemmelsene.

15.2. Informasjonssikkerhet

Datatilsynets oppfatning er at lovens § 13 i hovedsak er dekkende for de krav som bør stilles i loven.

I spørsmålet om hvorvidt det bør inntas et krav til kvalitet i informasjonssikkerhets-bestemmelsen, er Datatilsynet enig med departementet i at dette neppe vil tilføre bestemmelsen noe nytt. Etter Datatilsynets vurdering er det tilstrekkelig at dette fremkommer av bestemmelsen om internkontroll i § 14. Tilsynet mener imidlertid at det vil være

hensiktsmessig med like bestemmelser i helseregisterloven og personopplysningsloven. Dette bør avhjelpes ved å endre helseregisterlovens § 16.

15.3. Hjemmel til å utarbeide forskriftsbestemmelser om informasjonssikkerhet

Forskriftshjemmelen i personopplysningslovens § 13 lyder "Kongen kan gi forskrift om informasjonssikkerhet ved behandling av personopplysninger, herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak."

Det har i ulike sammenhenger blitt anført at dagens forskriftsregulering i personopplysningsforskriftens kapittel 2 går lenger enn det lovens § 13 åpner for.

De kravene som stilles forskriften, er etter Datatilsynets syn nødvendige for å ivareta en tilfredsstillende informasjonssikkerhet, og tilsynet er av den oppfatning at dagens forskriftsregulering er innenfor forskriftshjemmelens rammer, men anbefaler at dette vurderes, og at hjemmelsbestemmelsen eventuelt utvides, slik at regulering i forskrift på dagens nivå kan videreføres.

15.4. Forholdet mellom behandlingsansvarlig og databehandler

Tilsynets erfaring er at svært mange virksomheter benytter databehandlere, men forholdet mellom den behandlingsansvarlige og databehandleren er imidlertid sjelden regulert tilfredsstillende hos virksomhetene. Datatilsynet antar at dette delvis skyldes at innholdet i bestemmelsen er vanskelig tilgjengelig og at begrepet "databehandler" neppe er intuitivt for de behandlingsansvarlige. Etter Datatilsynets vurdering er det derfor hensiktsmessig å omformulere bestemmelsen slik at den behandlingsansvarlige lettere kan forstå hvilke plikter som følger av loven.

Bestemmelsen har som utgangspunkt at den behandlingsansvarlige kan stille de betingelser som anses som formålstjenlige. En databehandler tar et oppdrag fra en behandlingsansvarlig, og det er derfor naturlig å anta at det er den behandlingsansvarlige som bestemmer rammene for avtalen. Bestemmelsen i § 15 synes å bygge på en slik forestilling, men Datatilsynet erfarer at det ofte ikke er tilfellet. En databehandler vil ofte arbeide for standardiserte løsninger, hvor det er lite rom for individuelle tilpasninger for de enkelte kundene, og hvor slike tilpasninger vil medføre vesentlige merkostnader for den behandlingsansvarlige. Datatilsynet har bl.a. sett dette når det gjelder forholdet mellom de store skjemaleverandørene og kommunene. Konsekvensen vil kunne være at den behandlingsansvarlig har vansker med å fremme sine krav i avtalen. Datatilsynet har sett eksempler på at databehandlere søker å overprøve den behandlingsansvarliges vurdering av hvilke krav som bør stilles til informasjonssikkerheten. Dette er særlig uheldig der databehandleren er den sterke part i et avtaleforhold, og har utarbeidet standardvilkår som innebærer en aksept for et lavere sikkerhetsnivå enn det den behandlingsansvarlige anser som tilfredsstillende.
Forholdet kan til dels avhjelpes ved å klargjøre databehandlerens rolle i loven.

Etter Datatilsynet vurdering fremstår § 15 som en lite pedagogisk bestemmelse. En innledende positiv regulering av behandlingsansvarliges plikt til å etablere en

databehandleravtale, fremfor dagens innledning som omtaler forbud mot å behandle personopplysninger uten avtale med databehandleren, vil klargjøre bestemmelsen. Det fremstår også som noe uklart hvorfor behandlingene i bestemmelsens første ledd, annet punktum er nevnt særskilt.

Datatilsynet støtter synspunktet i utredningen om at databehandlerens oppgaver med fordel kan komme klarere fram i personopplysningsloven. Dette gjelder eksempelvis for den registrertes rett til informasjon. En slik klargjøring vil etter Datatilsynets vurdering tildels avhjelpe problemet med at styrkeforholdet i mange databehandlerrelasjoner er snudd; databehandleren vil vanskeligere kunne presentere avtalevilkår som er i strid med personopplysningsloven.

Tilsynet slutter seg også til departementets vurdering av hvilke momenter som er sentrale for å klargjøre bestemmelsen; det bør komme klarere frem når en databehandleravtale skal inngås samt på et overordnet nivå angis hva en slik avtale må inneholde. Det sistnevnte innebærer bl.a. at den behandlingsansvarliges rett og plikt til å stille krav til databehandlere må komme klarere fram. Dette gjelder både hvordan sentrale krav til internkontroll skal oppfylles, for eksempel innsyn, retting og sletting, men også hvordan informasjonssikkerheten skal ivaretas. Datatilsynet bemerker for øvrig at det fremstår som uklart hvor langt dokumentasjonsplikten i dagens § 14 annet ledd annen punktum rekker overfor databehandlere.

Mer konkrete bestemmelser om hvordan en databehandleravtale skal eller kan utformes bør skje i forskrift og gjennom veiledning. Datatilsynet har nylig utformet en veileder om utforming av databehandleravtaler.

16. Forholdet mellom personopplysningsloven og personopplysningsforskriften – særlig om behovet for særregulering av kredittopplysningsvirksomhet

Personopplysningslovens § 3 fjerde ledd åpner for at det kan gis nærmere regler for kredittopplysningsvirksomhet i forskrift. Slik regulering følger i dag av personopplysningsforskriftens kapittel 4. Bestemmelsene i kapittel 4 regulerer blant annet utlevering av kredittopplysninger, gjenpartsplikt og konsesjonsplikt.

Det følger av personopplysningsforskriftens § 4-5 at det kreves konsesjon fra Datatilsynet for å drive kredittopplysningsvirksomhet. Kredittopplysningskonsesjonen gir detaljerte regler og vilkår for bruk av kredittopplysninger. I praksis er konsesjonen en såkalt standardkonsesjon, som er lik for alle kredittopplysningsbyråene som får tillatelse til å drive kredittopplysningsvirksomhet. Per i dag har åtte virksomheter konsesjon fra Datatilsynet.

Det særegne med reguleringen av kredittopplysningsvirksomhet, jf. personopplysningslovens § 3 fjerde ledd og personopplysingsforskriftens § 4-1 annet ledd, er at personopplysningsloven og reglene om kreditopplysningsvirksomhet også gjelder for behandling av kredittopplysninger om andre enn enkeltpersoner. Utvidelsen av personopplysningsregelverkets rekkevidde på dette området er begrunnet med at også næringsdrivende vil ha et behov for vern. Utrederne fremhever at unntaket fra avgrensningen mot juridiske personer på dette området kommer i konflikt med ønsket om å renskjære

personopplysningslovens saklige virkeområde. Det understrekes likevel at det er ønskelig at juridiske personer gis et vern i forbindelse med kredittopplysningsvirksomhet. I utredningen anbefales det at en bestemmelse tilsvarende forskriftens § 4-2 annet ledd plasseres i annen lovgivning.

Det finnes lovgivning på kredittopplysningsområdet både i Sverige og Finland. I Sverige er det et flersporet system som i Norge, med både lovregulering, forskriftsregulering og krav om konsesjon fra Datainspektionen for gitte typer kredittopplysningsvirksomhet. Den svenske "kreditupplysningslagen" (1973:1173) og "kreditupplysningsförordningen" (1981:955) går imidlertid lenger enn personopplysningsforskriftens kapittel fire i å klargjøre hvordan behandlingen av personopplysninger kan skje.

Kredittopplysningsforetakene har i praksis overlatt mye av ansvaret for lovligheten av kredittvurderinger til etterspørrerne av opplysninger, i forhold til når kredittvurderinger kan innhentes, hvilke opplysninger som er nødvendig i den forbindelse og hvor lenge vurderingene kan lagres. Særlig gjelder dette vurderingen av det utløsende kravet om et saklig behov i forskriftens § 4-3 første ledd. Etterspørrer har imidlertid mangelfulle forutsetninger for å vurdere disse spørsmålene, all den tid bestemmelsene i personopplysningsforskriftens kapittel 4 og standardkonsesjonen retter seg mot kredittopplysningsforetakene.

Av Ot. Prp. nr. 92 (1998-99) fremgår det imidlertid av punkt 7.5 at "departementet er av den vurdering at reglene om kredittvurdering på sikt bør lovreguleres, enten som del av den nye personopplysningsloven eller ved en egen lov om behandling av kredittopplysninger."

Datatilsynet støtter konklusjonen om reguleringen av kredittopplysningsvirksomhet bør plasseres i en egen lovgivning eller forskrift. Tilsynets erfaring viser at det ikke fremstår som naturlig for etterspørrere av kredittopplysninger om juridiske personer, å gjøre seg kjent med de særegne bestemmelsen i personopplysningsregelverket på dette området. Flere materielle regler vil gjøre forutberegnligheten bedre. Særlig gjelder det for den store gruppen av etterspørrere av kredittvurderinger, som også vil ha plikter og rettigheter i forbindelse med innhenting av kredittopplysninger, eksempelvis det nevnte kravet til saklig behov og oppbevaring og sletting av opplysningene. Per i dag er etterspørrerne avhengig av tilfredsstillende informasjon fra kredittopplysningsvirksomheten for å opptre i tråd med reguleringen. Datatilsynets erfaring har vist at denne informasjonsoverføringen til en viss grad svikter.

Datatilsynet er imidlertid uenig i utredernes utgangspunkt for plassering av et eventuelt kredittopplysningsregelverk i bank- og finanslovgivningen. Tvert i mot er Datatilsynet av den oppfatning at det er svært viktig at tilsynet bevarer kontrollen med bruk av kredittvurderinger og kredittopplysningsvirksomhetene. Både mengden av personopplysninger som behandles gjennom denne typen virksomhet og det faktum at opplysningene oppleves som følsomme, tilsier at Datatilsynet som et uavhengig forvaltningsorgan tillegges denne oppgaven. Tilsynet har videre lang erfaring med regulering av denne type virksomhet.

16.1. Behov for å innskrenke adgangen til å innhente kredittopplysninger

Det gjennomføres i dag omtrent 25 millioner kredittvurderinger årlig, og majoriteten av disse er kredittvurderinger av enkeltpersoner. Fremgangsmåten for innhenting av opplysningene har i stor utstrekning endret seg fra skriftlig formidling, via brev, til virksomheters online tilgang til kredittopplysningsbyråenes databaser. Den faktiske utviklingen er ikke fulgt opp med endringer i lovverket, noe som medfører at store deler av kapittel 4 i personopplysningsforskriften, som regulerer kredittopplysningsvirksomhet særskilt, er utdatert. Datatilsynet har forsøkt å fange opp noe av utviklingen gjennom regulering i standardkonsesjonen til kredittopplysningsbyråene, men dette er etter tilsynets oppfatning ikke tilstrekkelig.

Særlig nevnes her grunnkravet til å foreta en kredittvurdering, jf. personopplysningsforskriftens § 4-3 første ledd som stiller krav om at det må foreligge et saklig behov for vurderingen. I utgangspunktet vil det foreligge et saklig behov i de tilfeller det skal inngås en avtale som innebærer et element av kreditt. Praksis har over tid utviklet seg dit hen at det per i dag vil fremstå som saklig å foreta en kredittvurdering hvor kredittelementet ligger i overkant av 200 kroner. Etter Datatilsynets vurdering er det nødvendig å stramme inn på denne praksisen, og da fortrinnsvis gjennom en nærmere regulering av kravet til saklig behov.

17. Elektroniske spor

Den teknologiske utviklingen har medført at vi legger igjen stadig flere såkalte "elektroniske spor". Datatilsynet har ved overgangen fra manuelle til elektroniske systemer registrert et ønske om å bruke elektroniske spor knyttet til identitet. En rekke av disse sporene er unødvendige å registrere i første omgang – eller unødvendig å lagre. På mange områder har utviklingen medført at adgangen til å være anonym har blitt illusorisk. Erfaringen viser at der elektroniske spor først lagres, er det et press om å benytte disse til andre formål. Aktuelle eksempler er lagring av IP-adresser i forbindelse med privat etterforsking av fildelere på Internett, debatten rundt datalagringsdirektivet, innføring av nye elektroniske billettsystem og de nye forskriftsbestemmelsene om arbeidsgivers rett til innsyn i ansattes e-post mv.

Datatilsynet viser til at Regjeringen og Stortinget gjentatte ganger har reist spørsmål rundt retten og muligheten til å være anonym. I St.meld. St.meld. nr. 17 (2006-2007) "*Eit informasjonssamfunn for alle*" gikk regjeringen inn for at det fremdeles måtte være tilbud om anonyme løsninger i sammenhenger der det ikke er nødvendig å identifisere seg. Dette ble fulgt opp av Stortinget i Innst. S. nr. 158 (2006-2007). Her pekte Transport- og kommunikasjonskomiteen på at "retten til å være anonym i utgangspunktet gjelder overalt, både på vegene, når man snakker i telefonen eller når man surfer på Internett". Retten til anonymitet er fulgt opp av Personvernkommisjonen i NOU 2009: 1, bl.a. i forbindelse med behandlingen av personvern i transportsektoren.

17.1. Datatilsynets vurdering av de foreslåtte endringer

Datatilsynet deler oppfatningen om at problematikken rundt elektroniske spor i stor grad kan løses gjennom de alminnelige bestemmelsene i personopplysningsloven. Ved behov kan imidlertid registrering og bruk av elektroniske spor reguleres særskilt slik det er gjort i personvernforskriften når det gjelder arbeidsgivers innsyn i ansattes e-post mv. Datatilsynet går ikke her nærmere inn på hvilke andre situasjoner dette kan være aktuelt for.

Videre bør de klare utsagnene fra regjeringen og Stortinget om rett til anonymitet, kunne få betydning for håndhevelsen av loven. Utsagnene bør eksempelvis kunne legge føringer for hvilke krav som skal stilles til sletterutiner etter lovens § 28, mulighet for kobling av personopplysninger etter § 11 jf. §§ 8 og 9 samt informasjonsplikten etter §§ 19 og 20.

18. Straffebestemmelsen i personopplysningslovens § 48

Etter Datatilsynets vurdering er straffebestemmelsene til dels problematiske fordi så få virksomheter kjenner til lovens krav. Det fremstår også som noe uheldig at en mindre alvorlig krenkelse av personvernet, eksempelvis brudd på meldeplikten, er straffesanksjonert, mens mer grove overtramp ikke er det. Dette gjelder for eksempel behandling av personopplysninger uten tilstrekkelig behandlingsgrunnlag i §§ 11 jf. § 8. Datatilsynet ser imidlertid at det kan være vanskelig å straffesanksjonere mer skjønnsmessige bestemmelser. Etter Datatilsynets vurdering kan imidlertid § 48 med fordel gjennomgås på nytt, med særlig henblikk på hvilke overtredelser som er straffesanksjonert, herunder hvorvidt disse bestemmelsene er formulert klart nok til at det er lett å påvise et brudd på regelverket og at hensynet til foruberegnelighet ivaretas.

19. Administrative og økonomiske forhold – med henblikk på meldingsdatabasen og kameraovervåkning

Etter tilsynene med kameraovervåkning som har funnet sted de senere årene kan tilsynet konstater at mange behandlingsansvarlige ikke følger loven innenfor dette området. Datatilsynets elektronisk meldingsdatabase består til enhver tid av samtlige meldinger som er sendt inn de tre foregående år.

Datatilsynet ser imidlertid at det er behov for en mer fullstendig oversikt over det totale omfenget av kameraovervåkning i samfunnet. Dette vil kunne oppnås ved at meldesystemet utvides for melding som gjelder slik overvåkning gjennom å kreve at meldingene inneholder mer detaljerte opplysninger enn i dag.

Vi mener at dagens regelverk gir mulighet for en slik løsning, men å bygge ut meldingsdatabasen vil kreve en betydelig del av de ressurser Datatilsynet har til rådighet. Tilsynet har sett på hva som kan være en mulig fremgangsmåte for å få en bedre oversikt over omfanget av bruk av overvåkningskameraer. Blant annet kan unntaket fra meldeplikten for virksomheter med personvernombud oppheves på dette punkt, slik at informasjon om all kameraovervåkning som omfattes av loven sentraliseres hos tilsynet.

Videre kan vi etterspørre ytterligere detaljer om overvåkningen:

- Formål med kameraovervåkingen
- Antall kameraer
- Tekniske spesifikasjoner (lydopptaksmuligheter, zoom-funksjon, IP-funksjonalitet, lagring eller monitorering mv)
- Geografisk posisjon (gateadresse, og/eller gps-koordinater).

En slik detaljert melding med henhold til antall kameraer, geografisk lokalisering med videre, vil gi Datatilsynet en mulighet til å visualisere overvåkingstrykket i Norge ved hjelp av karttjenester, og som statistikk knyttet til de enkelte fylker og kommuner. Det er mulig at en slik detaljeringsgrad foranlediger endringer i personopplysningsforskriften, men denne problemstillingen må utstå til senere all den tid vi ikke har prioritert dette i forbindelse med høringen om personopplysningsloven. Praksis i dag er knyttet til den behandlingsansvarlige og dersom det for eksempel er en butikkjede som benytter overvåkning i alle sine forretninger vil dette kun resultere i én melding til Datatilsynet. For å kunne presentere oversikter som beskrevet over er tilsynet avhengig av at det sendes inn en melding for hver fysiske lokasjon, slik at oversikten gir et mer korrekt bilde av hvor det er overvåkningskameraer.

Ettersom loven krever at meldinger fornyes hvert tredje år vil det minst ta tre år før tilsynet vil kunne presentere en slik detaljert oversikt. Som påpekt vil dette kreve ressurser i oppstartsfasen, samt over tid. I tillegg til kostnader forbundet med etablering av en ny praksis og investering i infrastruktur – programvare og internettfunksjonalitet – er det påregnelig at det vil bli behov for en personellmessig styrking for å gjennomgå de meldingene som kommer inn.

Med hilsen

Georg Apenes
direktør

Hågen Ljøgodt
rådgiver

Kopi: Fornyings- og Administrasjonsdepartementet, v/Statsforvaltningsavdelingen, Pb 8004 Dep, 0030 Oslo

Vedlegg:

1. Høringsuttalelse - NOU 1:2009 Individ og integritet
2. Datatilsynets rapport om kameraovervåkning fra 2005
3. Datatilsynets brev til Justisdepartementet om kameraovervåkning av 19. mai 2009