DET KONGELIGE FORNYINGS-
OG ADMINISTRASJONSDEPARTEMENT

Justis- og politidepartementet
Postboks 8005 Dep
0030 OSLO

Deres referanse	Vår referanse	Dato
200904400 ES HAJ/mk	200901925-/AKH	02.02.2010

Høring – etterkontroll av personopplysningsloven

Vi viser til Justisdepartementets (JD) brev av 03.07.2009 vedlagt høringsnotat med vedlegg om etterkontroll av lov om behandling av personopplysninger 14.04.2000 nr. 31 (pol). Fornyings- og administrasjonsdepartementet (FAD) har gjennomgått dokumentasjonen, og har strukturert merknadene etter kapittelinndelingen i JDs høringsnotat.

Innledende merknader

I forbindelse med etterkontrollen har JD og FAD (daværende Moderniseringsdepartementet) gitt oppdrag om å utrede behovet for endringer i personopplysningsloven til Dag Wiese Schartum og Lee Bygrave ved Universitetet i Oslo. De har levert to omfattende delutredninger, hvorav den ene gjelder behandling av personopplysninger generelt (heretter kalt rapport I), mens den andre kun gjelder behandling av biometriske opplysninger og fødselsnummer (heretter kalt rapport II). Rapportene er grundig gjennomarbeidet, og gir etter vår vurdering et godt utgangspunkt for revisjon av personopplysningsloven. I tillegg inneholder etterkontrollen en rapport om fjernsynsovervåking utarbeidet av Datatilsynet.

Personopplysningsregelverket inneholder rettigheter som skal beskytte samtlige borgeres private sfære og personlige integritet. Reglene bør derfor kunne leses og forstås av flest mulig. Dette legger også utrederne til grunn i rapport I s. 12, der de uttaler at en lov som henvender seg til folk flest i størst mulig grad bør gi full informasjon. Vi mener likevel at en del av de foreslåtte lovendringene vil være vanskelig å forstå for befolkningen. Utrederne har lagt til grunn at flest mulig bestemmelser bør

Postadresse
Postboks 8004 Dep
N-0030 OSLO

Kontoradresse
Akersg. 59

Telefon
22 24 90 90
Org no.
972 417 785

Administrasjonsavdelingen
Telefaks
22 24 27 14

Saksbehandler
Anne Kristine Hage
22 24 48 51

tas inn i loven. Dette har ført til et omfattende og til dels komplisert forslag. FAD er i tvil om dette er en god måte å nå frem med personvernbudskapet til befolkningen og de behandlingsansvarlige på. Som et konkret eksempel kan det radikale lovforslaget § 33a om konsesjonsplikt, se ut til å kunne gi grunnlag for svært omfattende saksbehandling. For øvrig vil vi understreke at rapportene inneholder grundige vurderinger som grunnlag for viktige interesseavveininger i arbeidet med regelendringsforslag. Vi finner også at JDs høringsbrev på en god måte synliggjør mange av de viktige vurderingene som bør foretas ved etterkontrollen av loven. Høringsbrevet er derfor godt egnet som støtte og supplement til de øvrige dokumentene i saken.

Innledningsvis viser vi også til våre merknader knyttet til sletting av opplysninger. Det er et faktum at mange behandlingsansvarlige tar vare på stadig flere personopplysninger over lang tid som følge av lave kostnader for slik lagring. Ytterligere merknader til denne problematikken er plassert i kapittel 4.

Våre merknader er hovedsakelig knyttet til JDs forslag til regelverksendringer, samt til utredernes radikale lovforslag. Vi mener at teksten i det radikale lovforslaget kan gjøres betydelig enklere og tydeligere. En del begreper og formuleringer bør byttes ut med mer allment tilgjengelige begreper.

FAD anbefaler også at lovutkastets paragrafnummerering forenkles i forhold til det som fremkommer i rapport I. Vi ser at det kan være ønskelig å beholde dagens nummerering på bestemmelser som ikke endres innholdsmessig, for å lette gjenkjennelse og gjenfinning av bestemmelsene. Den strukturen som nå er valgt, med f. eks. §§ 8, 8a, 8b etc. med flere bokstavinndelinger i hver paragraf, kan gjøre det vanskelig å henvise til bestemmelsene og dermed skape uklarhet. Det er videre vår vurdering at dersom man velger å følge opp det radikale lovforslaget, er endringene så omfattende i forhold til gjeldende lov, at endring i paragrafnummerering neppe vil være et stort problem. Brukerne må uansett sette seg inn i et "nytt" regelverk. Utfordringene med endret nummerering kan også avhjelpes ved et godt lovspeil. Vi oppfordrer derfor JD til å vurdere en enklere nummerering av regelverket enn det som fremgår av det radikale lovforslaget.

1. DEFINISJONER

Definisjonene i personopplysningsloven (§ 2)

Det er viktig at begrepsdefinisjonene i personopplysningsloven revurderes og drøftes kritisk på bakgrunn av de erfaringer som er høstet siden loven trådte i kraft. Samtidig er begrepene og definisjonene i personopplysningsloven godt innarbeidet. Det bør derfor foreligge vektige grunner for å endre begreper og definisjoner.

I utredernes og JDs forslag til endringer er det få holdepunkter fra praksis som viser behov for omfattende endringer av lovens begrepsdefinisjoner. Det vises heller ikke til

at eksisterende definisjoner er i strid med direktivets ordlyd, eller er villedende for etterlevelse av direktivet.

Endringer av begrepsdefinisjonene begrunnes til dels med hensynet til enhetlig språk innen de nordiske land. FAD er enig i at det er et viktig argument for å endre definisjonene. På den annen side oppfatter vi at det er viktigere å se på lignende definisjoner i vår egen lovgivning. Forvaltningsloven benytter noen av de samme begrepsdefinisjoner som i gjeldende personopplysningslov. Tilsvarende gjelder også for helseregisterloven og helseforskningsloven. Hensynet til mest mulig entydige begrepsdefinisjoner i nasjonalt lovverk bør etter vår oppfatning tillegges større vekt.

Begrepet "personopplysning"

"Enkeltperson"

Med unntak av reglene om kredittopplysningsvirksomhet i personopplysningsforskriften § 4-2, omfattes kun opplysninger om "fysiske personer" av personopplysningsloven. Dette følger både av ordlyden "enkeltperson", og av forarbeider og rettspraksis. I visse tilfeller kan det være tvil om opplysninger om en juridisk person kan knyttes til en fysisk person. Dersom det eksisterer en slik tilknytning til en enkeltperson, vil opplysningen om den juridiske person være å anse som personopplysning. Å tilføye *"fysisk"* før "enkeltperson" medfører etter vår vurdering ikke større klarhet på dette punkt. Begrepsdefinisjonen "enkeltperson" er godt innarbeidet, også i annen lovgivning. Som eksempel viser vi til følgende bestemmelser:

> Forvaltningsloven § 2:
> "a) .....bestemmende for rettigheter eller plikter til private personer (*enkeltpersoner* eller andre private rettssubjekter)"
>
> Helseregisterloven § 2:
> "helseopplysninger: taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en *enkeltperson"*

Ingen av bestemmelsene benytter begrepet "fysisk person". Som vist ovenfor legger helselovgivningen flere av personopplysningslovens begrepsdefinisjoner til grunn. Ensartede begrepsdefinisjoner er nyttig for dem som må forholde seg til flere lover samtidig. Begrepene "fysisk" contra "juridisk" person oppfatter vi er en distansering fra alminnelig språkbruk og representerer et mer rendyrket juridisk språk. Vi mener det ikke er dokumentert forhold som gjør det nødvendig å endre innarbeidete begreper. Vi anbefaler derfor å beholde begrepsdefinisjonen "enkeltperson" slik loven lyder i dag.

"opplysninger og vurderinger"

Vi viser generelt til våre merknader til foregående avsnitt, jf. gjengivelsen fra andre lover. Den foreslåtte endring fra "opplysninger og vurderinger" til "informasjon", kan føre til at "vurderinger" ikke omfattes. De som er fortrolig med dagens regler kan

oppfatte endringen slik at "vurderinger" ikke lenger er omfattet. Begrepet "informasjon" kan favne videre enn den gjeldende definisjon. Vi oppfatter dette begrepet som mindre presist. Hoveddefinisjonen av "personopplysning" bør derfor bli stående slik den er i dag. Dersom gode grunner taler for det kan § 2 nr. 1, utvides med de tillegg som oppfattes å være nødvendig.

For eksempel: Opplysninger om en død person omfattes bare av denne loven hvis de kan knyttes til en person som er i live.

Særlig om humant biologisk materiale

FAD ser behovet for at loven omtaler biologisk materiale og i hvilken grad dette bør omfattes av begrepet "personopplysning". Det virker mer hensiktsmessig og tydelig at lovteksten presiserer når biologisk materiale er en "personopplysning" fremfor å avgrense negativt. En slik presisering vil vise til at det er de samme vurderinger for disse "opplysningene" som for de øvrige opplysningene som omfattes av personopplysningsbegrepet. Når det eksisterer en kobling/nøkkel til giver, er også biologisk materiale å oppfatte som personopplysninger. Er det derimot ikke mulig å koble identitet og det biologiske materialet er det ikke en personopplysning. Det er interessant å se på omtale og regulering i helselovgivningen:

Lov om behandlingsbiobanker § 3, andre ledd:
"Med mindre annet følger av denne loven, skal *helse- og personopplysninger som utledes fra humant biologisk materiale* behandles etter personopplysningsloven, helseregisterloven, helsepersonelloven og eventuelt annen lovgivning som særlig regulerer vern av personopplysninger."

Helseforskningsloven § 20:
"Samtykke kreves ikke ved bruk av *anonymisert humant biologisk materiale* og anonyme opplysninger. For innhenting av materiale og opplysninger som senere skal anonymiseres, kreves det samtykke etter kapitlet her."

Fra forarbeidene i Ot.prp. nr. 74 (2006-2007) Om lov om medisinsk og helsefaglig forskning (helseforskningsloven) uttales det i innledningen til pkt. 12.8.1: "I dette punktet redegjøres det for forholdet mellom samtykkekravet og anonymt humant biologisk materiale og anonyme opplysninger. Materiale og opplysninger vil være anonyme dersom fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene eller materialet ikke lenger kan knyttes til en enkeltperson."

I lov om behandlingsbiobanker omtales bare det som utledes av materialet som opplysninger, mens helseforskningsloven likestiller materialet som sådan med opplysninger, så lenge materialet kan knyttes til en enkeltperson. I de fleste sammenhenger eksisterer ikke biologisk materiale uten en tilknytning til giver/pasient. Biologisk materiale er i økende grad en av de mest innholdsrike og interessante informasjonsbærere om enkeltindivid, slekt og samfunn. Hovedinnholdet i

opplysningene som kan utledes fra biologisk materiale vil være sensitive. De fleste biologiske prøver vil også inneholde langt mer sensitiv informasjon enn avgiveren har forutsetninger for å forstå. Biologisk materiale fra døde vil også inneholde personopplysninger om helseforhold som angår gjenlevende slektninger. FAD foreslår av den grunn følgende formulering: "*Biologisk materiale er personopplysninger bare når det kan knyttes til en enkeltperson.*"

Kravet om identifikasjon

Personvernnemndas praksis har løftet frem viktige problemstillinger som bør avklares. En slik problemstilling kommer til uttrykk i PVN-2005-12 om at videoopptak ikke er å anse som personopplysninger før det blir avspilt. Vi kan se at lovens nåværende formulering er uheldig og kan danne grunnlag for en slik tolkning. Ut fra artikkel 29-gruppens tolkning av "identifiable person" i personverndirektivet art. 2 a), er det ikke nødvendig at identifisering har skjedd så fremt identifisering er mulig.

Vi oppfatter at utrykket "som kan knyttes til" er i samsvar med direktivets krav til identifikasjon og samtidig godt og enkelt uttrykt på norsk. Når intensjonen er at begrepet skal omfatte mer enn praksis viser i dag, anbefaler vi at den eksisterende ordlyden gis et tillegg som underbygger artikkel 29-gruppens fortolkning.

FAD foreslår følgende ordlyd: "som det er mulig å knytte til en enkeltperson". Dette synes å være mest i samsvar med direktivteksten: "identifiable".

Pseudonymisering

Etter artikkel 29-gruppens uttalelser, er det rimelig klart at behandling av pseudonymiserte opplysninger er å anse som personopplysninger. FAD er imidlertid enig i JDs vurdering av at dette ikke er til hinder for at det inntas enkelte unntak for slike opplysninger i personopplysningsloven. En slik behandling vil representere en mindre personvernmessig risiko.

Å tilgodese personvernvennlige lagringsalternativer kan være et viktig virkemiddel for å begrense unødvendig lagring av direkte identifiserbare personopplysninger, for eksempel ved å lempe på noen av kravene når opplysningene er pseudonyme, herunder samtykke. Spørsmålet må ses i sammenheng med den øvrige regulering, så som rapporteringsplikt om hvilke opplysninger som inngår, slik at det er mulig å føre tilsyn med at pseudonymiseringskravet faktisk overholdes. Ofte oppgis bare hovedinnholdet i form av type eller kategori av opplysninger, der hver slik "kategori" kan inneholde både mange og detaljerte opplysninger som kan røpe de registrertes identitet.

Det er tydelig at begrepet "pseudonym" oppfattes flertydig, og at det er behov for å avklare begrepsinnholdet. Når det er ønskelig å vektlegge begreper som omfatter ulike måter å lagre personopplysninger på, bør slike begreper defineres på en mest mulig entydig måte i loven. Når det synes å være klare holdepunkter for at innholdet i

begrepet "pseudonymt" er problematisk, mener vi at det er lite heldig å lansere grader av begrepet, så som "streng" pseudonymisering.

Intensjonen med pseudonymet er at det skal være en personvernvennlig måte å lagre opplysninger på, og som likevel gjør det mulig å følge enkeltindivider over tid. Dette er også mulig med såkalt avidentifiserte opplysninger. Pseudonyme og avidentifiserte opplysninger har det til felles at de fremstår som anonyme på mottakers hånd. Det vil si at mengde- og detaljeringsgrad på opplysningene må behandles forut for utleveringen. Som hovedregel vil dette innebære at antallet opplysninger kan være betydelig redusert på mottakers hånd sammenlignet med de opprinnelige opplysningene som finnes hos avgiver. Hovedforskjellen mellom de to oppbevaringsmåtene er hvor vanskelig eller enkelt det er å få tilgang til identiteten til den personen opplysningene er knyttet til. For de avidentifiserte opplysningene oppbevares identitetsopplysningene adskilt fra de øvrige opplysningene, ev. ligger nøkkelen til identiteten hos den som har utlevert opplysningene. For pseudonyme opplysninger er nøkkelen utilgjengelig for både avgiver og mottaker fordi det er en uavhengig tredjepart som har nøkkelen. Tredjeparten har bare nøkkel og ingen opplysninger. Vi anbefaler at det utarbeides definisjoner av anonyme, avidentifiserte og pseudonyme personopplysninger i loven. I tillegg vil det være nødvendig med en forskriftshjemmel for utdypende regulering.

Sensitive opplysninger

Uttrykket "opplysningstype" bør ikke tas inn i definisjonen av sensitive personopplysninger. Men vi ser behovet for å supplere lovteksten slik at den tydeliggjør at all informasjon som kan avdekke et av de nevnte sensitive forhold, er å anse som sensitiv. Dette er viktig for å få frem at sammenstilling av ellers trivielle opplysninger, samlet sett kan gi sensitiv informasjon. Det kan også vurderes om "taushetsbelagte opplysninger" bør tas inn som en selvstendig definisjon av "sensitive opplysninger". Dette kan forenkle grensedragningene for hva som skal omfattes.

FAD foreslår at "åpenbare" byttes ut med ordet "avdekke". "Avdekke" er etter vår mening et enklere begrep å forstå. Vi anbefaler også at kravet til en slik vurdering bør skjerpes ved å sette ordet *kan* foran.

Alternative forslag til ordlyd

Personopplysning: opplysninger og vurderinger som det er mulig å knytte til en enkeltperson.

Opplysninger om en død person er bare personopplysninger hvis de kan knyttes til en enkeltperson som er i live.

Biologisk materiale er personopplysninger bare når det kan knyttes til en enkeltperson.

Sensitive personopplysninger: opplysninger og vurderinger som kan avdekke:

Begrepet "behandling av personopplysning"
Vi er enig i at behandlingsbegrepet i personopplysningsloven kan være flertydig og av og til skape tolkningsproblemer. I likhet med JD ser vi likevel ikke at disse uklarhetene løses ved enkle endringer i lovens definisjoner. Vi anbefaler derfor å beholde dagens definisjon.

Begrepet "personregister"
Gjenfinningskriteriet er innarbeidet som et vilkår for å regne noe som et personregister. Dette kommer tydeligst frem gjennom praksis, men følger også etter FADs mening av ordlyden i dag, jf. "slik at opplysningene om den enkelte kan finnes igjen" i pol. § 2 nr. 3). Vi er enig med JD i at "registre, fortegnelser mv." bør erstattes med "en samling av personopplysninger". Vi anbefaler at ordet "systematisk" utgår fra definisjonen, da innholdet i gjenfinningskriteriet ivaretas av begrepet "på en slik måte at".

Vi foreslår følgende definisjon av personregister:
"personregister: samling av personopplysninger lagret på en slik måte at opplysninger om den enkelte kan gjenfinnes."

Begrepet "behandlingsansvarlig"
Behandlingsansvaret er sentralt for etterlevelse og mulig sanksjonering av loven, herunder mulighet for å saksøke den ansvarlige. Definisjonen av den behandlingsansvarlige bør samtidig være mest mulig sammenfallende med det alminnelige virksomhetsansvaret. Virksomhetsansvaret ligger hos virksomhetens ansvarlige leder eller øverste leder. Selv om en definisjon i utgangspunktet ikke bør benytte de samme ord som inngår i det begrepet som skal defineres, mener vi "ansvar" er bedre enn "bestemme". JD bør vurdere å endre formuleringen til at den behandlingsansvarlige er virksomhetens øverste leder og er ansvarlig for å sikre at formål med og behandlingsprosedyrer for personopplysningene er i samsvar med loven. Deretter kan det vises til bestemmelsene der pliktene finnes.

JD foreslår å ta inn en henvisning til at behandlingsansvarlige kan være angitt direkte i hjemmelsloven. Dette er blant annet gjort i helseregisterloven i dag. FAD er enig i at dette kan være nyttig, men finner likevel grunn til å peke på at dette nok bare er praktisk for større, offentlige registre.

2. PERSONOPPLYSNINGSLOVENS SAKLIGE VIRKEOMRÅDE

Også her har Personvernnemda brakt opp en problemstilling som krever en avklaring. Nemndas avgjørelse 2005-01, gjelder et lydbåndopptak av en telefonsamtale, og om et slikt opptak ligger innenfor lovens virkeområde. Nemnda synliggjør en inkonsistens mellom lovens ordlyd og forarbeidene. Justisdepartementet mener at PVNs fortolkning av pol § 3 litra a innsnevrer lovens virkeområde i forhold til direktivets ordlyd og de

øvrige EU/EØS- lands praksis. En annen praksis enn den nemnda har lagt til grunn i avgjørelsen 2005-01, taler derfor for en lovendring.

FAD mener at personopplysningsloven mister mye av sin slagkraft dersom all manuell elektronisk behandling, faller utenfor loven. Lovteksten bør endres i tråd med dette. FAD støtter JDs forslag om følgende ordlyd; "helt eller delvis skjer automatisert med elektroniske hjelpemidler". Denne ordlyden åpner for at også delvis manuelle elektroniske behandlinger omfattes. Dette synes å definere lovens virkeområde slik regelen tolkes i Norden og i øvrige EU- land.

Personopplysningsloven § 3, annet ledd

Justeringer av dagens ordlyd

Utrederne foreslår ny ordlyd i personopplysningsloven § 3, annet ledd, hvor fokus flyttes fra formålet med behandlingen til behandlingens karakter. Bakgrunnen for justering av bestemmelsen er at den bedre skal harmonere med avgjørelser fra EU-domstolen om forståelsen av EU-direktivet på dette punktet, bl.a. Lindqvistdommen. FAD er enig med JD i at dagens formulering i § 3, annet ledd, hvor unntaket knyttes til "personlige" eller andre "private" behandlinger, på en god måte får frem det familieaspektet som direktivet antyder. FAD mener begrepet "aktiviteter" ikke er mer klargjørende enn "formål". Formålsbegrepet er godt innarbeidet og bør derfor beholdes. Samtidig foreslår vi å ytterligere understreke det personlige og private ved å bytte ut "rent" med "utelukkende". FAD foreslår derfor følgende ordlyd:

> "Loven gjelder ikke behandling av personopplysninger som den enkelte *utelukkende* foretar for personlige eller andre private formål."

I tillegg bør det føyes til et ledd som presiserer at kameraovervåking faller innenfor lovens virkeområde. Vi foreslår følgende lovtekst:

Loven gjelder for enhver form for kameraovervåking.

Særlig om publisering på Internett

Selv om publisering per definisjon betyr offentliggjøring for allmennheten, er det et faktum at man i dagligtale også snakker om publisering for en mindre/avgrenset krets av personer. Departementet foreslår at § 3, annet ledd, som slår fast at personopplysningsloven ikke gjelder for behandling av personopplysninger som foretas for personlige eller andre private formål, blir supplert med en regel som sier noe om i hvilken grad publiseringer på Internett kan skje uten at loven kommer til anvendelse. JD foreslår følgende tillegg til annet ledd:

"*Dette gjelder likevel ikke behandlinger som innebærer publisering av personopplysninger på Internett, med mindre det kun er en konkret og begrenset krets av personer som har tilgang til opplysningene.*"

FAD er enig i at en slik presisering kan være et nyttig supplement til bestemmelsen, og støtter JDs forslag til endret lovtekst.

3. YTRINGSFRIHET OG PERSONVERN

FAD deler JDs vurdering av at begrepet "opinionsdannende" i gjeldende personopplysningslov § 7, kan ha blitt benyttet som et selvstendig vurderingsgrunnlag for unntak fra personopplysningslovens regler, uten at dette var hensikten da bestemmelsen ble utformet. FAD støtter derfor forslaget om å fjerne "opinionsdannende" fra bestemmelsen. Det bør videre tilføyes en henvisning til ytringsfrihet. Dette er også i samsvar med dansk og svensk personvernlovgivning, og i JDs forslag i høringsbrevet pkt. 3.3.4. På denne måten tydeliggjøres den avveiningen som skal foretas mellom personvern og ytringsfrihet.

Vi er enig med utrederne i at det er et stort behov for informasjons- og opplæringsarbeid for å lære borgerne bedre nettvett. Målet må være å unngå mange av de ytringene som i dag skaper utfordringer i grenselandet personvern/ytringsfrihet. FAD har de siste årene gitt Datatilsynet betydelige ressurser til kampanjen "Du bestemmer". Kampanjen er blitt en stor suksess. Nå er Tilsynet også gitt prosjektmidler for å etablere en prøveordning med en tjeneste som skal bistå publikum med å fjerne krenkende ytringer på nett. Tjenesten kalles slettmeg.no, og er foreløpig et to-årig prøveprosjekt.

4. KRAV TIL RETTSLIG GRUNNLAG FOR BEHANDLING AV PERSONOPPLYSNINGER

Generelle merknader om sletting av personopplysninger

Vi savner et avsnitt om sletting av personopplysninger. Verken utrederne eller JD har foreslått endringer i personopplysningslovens regler om sletting av personopplysninger. Etter gjeldende rett, kan en registrert person ikke kreve å få opplysninger om seg selv slettet dersom den behandlingsansvarlige har et behandlingsgrunnlag og de registrerte opplysningene er korrekte. Som eksempel kan nevnes Findexas forsøk med publisering av fødselsdato i telefonkatalogen på nett, eller den nå nylig lanserte tjenesten iam.no som sammenstiller offentlig tilgjengelig informasjon om de registrerte og gjør informasjonen lett tilgjengelig på www.iam.no

Behandlingene av personopplysninger i de ovennevnte eksemplene har høyst sannsynlig et rettslig grunnlag (personopplysningsloven § 8f), og de registrerte opplysningene er riktige. Mange har reagert negativt på begge de nevnte behandlingene av personopplysninger, men er ikke gitt mulighet til å få slettet objektivt riktige opplysninger som de ikke ønsker skal ligge tilgjengelig på de aktuelle tjenestene. Selv om en behandling har behandlingsgrunnlag i loven, bør ikke den behandlingsansvarlige ha en ubegrenset rett til å behandle opplysningene. Vi er innforstått med at de foreslåtte bestemmelsene i det radikale lovforslaget §§ 8 – 8c) vil kunne redusere adgangen til å igangsette den type behandlinger som her er nevnt, og at behovet for sletteregler således også reduseres noe i forhold til dagens situasjon. Vi anbefaler likevel at det tas inn en bestemmelse som gjør det mulig å kreve slettet

opplysninger som den behandlingsansvarige ikke har behov for å lagre ut fra andre hensyn enn egeninteresse/kommersiell interesse.

En annen utfordring knyttet til sletting av personopplysninger er at det stadig blir billigere og enklere å lagre informasjon. Mange behandlingsansvarlige erfarer at det er rimeligere og mindre arbeidskrevende å lagre informasjon enn å slette i henhold til de regler som følger av personopplysningsloven. Særlig gjelder dette på regnskapsområdet, der det etter hvert finnes enorme mengder transaksjonsdata som følge av at mange kjøp foretas ved bruk av elektroniske betalingsmidler. Informasjon lagres tilsynelatende ukritisk, uavhengig av om opplysningen omfattes av bokføringsregelverkets lagringsplikter eller ikke. Ofte slettes heller ikke opplysningene etter at pliktig lagringstid er utløpt. Denne utfordringen bør synliggjøres i det radikale lovforslaget § 10, som regulerer forbud mot å behandle opplysninger det ikke lenger er saklig behov for. Vi tror bestemmelsen vil kunne styrkes ved bruk av ordet *sletting*, for å understreke at opplysninger faktisk skal slettes når den behandlingsansvarlige ikke lenger har saklig behov for dem.

Personopplysningsloven § 8 bokstav f brukes ofte som rettslig grunnlag for å behandle personopplysninger. I mangel av annet rettslig grunnlag for å behandle personopplysninger, har den behandlingsansvarlige, med grunnlag i denne bestemmelsen, foretatt en egen vurdering av sin interesse i å behandle personopplysninger veid mot de registrertes interesse i personvern. Ikke overraskende slår denne vurderingen, riktig eller uriktig, ofte ut i favør av den behandlingsansvarlige. FAD er enig med utrederne i at det er behov for å stramme inn adgangen til å anføre nødvendighetsgrunn som rettslig grunnlag for behandling av personopplysninger. Nødvendighetsgrunnen skal være en sikkerhetsventil, og ikke en hovedregel.

Skille primære vs. sekundære rettsgrunnlag

På spørsmål om det kommer klart nok frem i gjeldende § 8 at samtykke og lovregulering skal være de primære behandlingsgrunnlagene, mens bokstavene a til f skal være sekundære behandlingsgrunnlag, svarer utrederne at de mener det bør inntas et uttrykkelig skille mellom primære og sekundære rettslige grunnlag. Et slikt skille følger ikke av dagens lovtekst, men er forutsatt i forarbeidene, jf. Ot.prp. nr. 92 (1998-99) samt Personvernnemnda i PVN 2001-04, som det vises til i rapport I. Det er et faktum at virksomheters kjennskap til og kunnskap om personvernlovgivningen, er mangelfull. Det er mye å forvente at behandlingsansvarlige vil sette seg inn i forarbeider og avgjørelser fattet av Personvernnemnda for på den måten å skaffe seg nødvendig kunnskap om gjeldende rett. Behandling hjemles ofte i personopplysningsloven § 8 bokstav a – f, spesielt i sikkerhetsventilen i bokstav f. Ut fra dette mener FAD det er hensiktsmessig å tydeliggjøre skillet mellom primære og sekundære rettsgrunnlag direkte i loven. På denne måten tydeliggjøres vurderingene som den behandlingsansvarlige må foreta før en behandling kan settes i gang.

Lovhjemmel og samtykke som rettsgrunnlag
Rettssikkerhets- og forutberegnelighetsprinsipper tilsier at det primære grunnlaget skal være lovhjemmel eller samtykke fra den registrerte. At også behandling av opplysninger som den registrerte frivillig har gjort alminnelig kjent skal falle innenfor det primære rettsgrunnlaget, synes å ha mye for seg, da det til en viss grad kan sidestilles med samtykke fra den registrerte. Dette følger etter dagens oppbygning kun av § 9 om sensitive personopplysninger. Ut fra et "fra det mer til det mindre" prinsipp bør det også kunne gjelde for personopplysninger som ikke er av sensitiv karakter. Det som da gjenstår som sekundære rettsgrunnlag, er de resterende nødvendighetskriteriene ut fra angitte formål. Vi mener at det da er riktig å presisere at disse sekundære rettslige grunnlagene kun skal benyttes dersom det er umulig eller uforholdsmessig vanskelig eller ressurskrevende å oppfylle de primære rettslige grunnlag.

Behandling av opplysninger som den registrerte frivillig har gjort offentlig kjent, er ikke helt uproblematisk. Selv om opplysningene er kjent, vil den registrerte kunne reagere negativt på konteksten opplysningene behandles i. Opplysninger gjort tilgjengelig på nett, kan settes sammen på nye måter og danne grunnlag for å utlede ny informasjon som den registrerte kan oppleve som krenkende. Vi viser til det vi har sagt ovenfor om at det bør gis mulighet for den enkelte til å be om at også lovlig behandlede opplysninger slettes dersom den behandlingsansvarlige ikke kan dokumentere et særskilt behov for opplysningene.

Det er også knyttet utfordringer til barn og unges offentliggjøring av opplysninger om seg selv. Barn og unge er storbrukere av digitale medier, og deler ofte mye personopplysninger i ulike nettsamfunn, blogger etc, uten nødvendigvis å tenke over eller forstå konsekvensene av dette. Etter vår vurdering er det hensiktsmessig å knytte retten til å behandle opplysninger den unge selv har gjort offentlig kjent til barnets samtykkekompetanse jf. det radikale lovforslaget § 6a. Etter dette forslaget har barnet selvstendig samtykkekompetanse først ved fylte 15 år. Det vil likeledes være naturlig å si at opplysninger barnet har gjort offentlig kjent før fylte 15 år, ikke kan behandles videre med grunnlag i § 8a bokstav c. Dette vil kunne sies å være en naturlig fortolkning av § 8a bokstav c sammenholdt med § 6a. Vi mener dette bør kommer tydelig frem i forarbeidene til bestemmelsene.

I høringsbrevet pkt. 4.3.2 stiller JD spørsmål om det er behov for å presisere kravet til lovhjemmel som grunnlag for behandling av personopplysninger. Spørsmålet har oppstått som følge av at noen lovhjemler helt klart regulerer behandling av opplysninger, mens andre i større grad forutsetter at slik behandling skal finne sted. FAD er enig med utrederne i at det radikale forslaget § 8a bokstav a og b gjør hjemmelskravet tydeligere enn slik det er i dag. Vi forstår forslaget slik at hjemmelskravet fortatt er relativt. Dette innebærer at jo mer inngripende en personopplysningsbehandling er, jo strengere må kravet til lovhjemmel være. Dette følger også av legalitetsprinsippet. Det som dermed klargjøres ved den formuleringen utrederne har foreslått i ny § 8a bokstav a og b, er at hjemmel i lov også kan omfatte

lovregler som forutsetter behandling av personopplysninger, men uten at behandlingen kommer klart frem i loven. Hvor langt bokstav b rekker, må tolkes i lys av legalitetsprinsippet, og vurderes konkret i det enkelte tilfellet.

Avtale med den registrerte som rettsgrunnlag
Det radikale lovforslaget innebærer at skillet mellom sensitive og "ordinære" personopplysninger blir uten betydning ved vurdering av om en behandling har rettslig grunnlag. Dette betyr at de samme vurderingene må foretas for all behandling av personopplysninger. I forhold til dagens system innebærer forslaget først og fremst strukturelle endringer, da samme rettslige grunnlag som hovedregel kan benyttes både for sensitive og ordinære personopplysninger. I dag er det imidlertid ikke adgang til å behandle sensitive opplysninger på grunnlag av at de er nødvendige for å oppfylle en avtale med den registrerte, mens utredernes forslag åpner for at dette behandlingsgrunnlaget anvendes generelt. FAD mener at behandling av personopplysninger basert på at den behandlingsansvarlige skal oppfylle en avtale med den registrerte, er nær beslektet med behandling med grunnlag i samtykke. Det er derfor hensiktsmessig at dette grunnlaget kan benyttes til å behandle alle typer personopplysninger. Dette forutsetter en avtale som er så tydelig at den registrerte forstår betydningen av å inngå avtalen, tilsvarende kravene som stilles til samtykke jf. forslaget § 6. På enkelte områder gjelder det likevel viktige begrensninger i avtaleadgangen, for eksempel forsikringsselskapenes adgang til å behandle genetisk informasjon. Av pedagogiske hensyn bør dette synliggjøres i regelverket.

Nødvendighetsvurdering som rettsgrunnlag
Utrederne går videre inn for å stramme inn personopplysningsloven § 8 f da de mener den åpner for at behandlingsansvarlige kan vinne fram med et argument om interesseovervekt i nesten ethvert tilfelle. FAD mener det er ønskelig med en innstramming slik at det er andre enn den behandlingsansvarlige som avgjør om han har tilstrekkelig grunn til å behandle personopplysningene. Dette er samtidig forbundet med noen praktiske utfordringer. Det vil være lite effektivt at interesseavveiningen gjøres av Datatilsynet. Da vil det være bedre at den behandlingsansvarlige beholder kompetansen til å avgjøre spørsmålet selv, men basert på objektivt avgrensede kriterier. Det må komme klart frem på tilsvarende måte som i dag, at sensitive personopplysninger ikke kan behandles på bakgrunn av en skjønnsmessig nødvendighetsvurdering. Dette mener vi lovutkastet oppnår i § 8c bokstav b. Det vil bidra til å skjerpe bruken av denne sikkerhetsventilen når det presiseres at personvernulemper må kartlegges før behandlingen igangsettes. Vi mener videre det er viktig at lovutkastet gir Datatilsynet et bedre grunnlag for å kontrollere at behandlingen av personopplysninger skjer i tråd med lovgivningen, uten at behandlingsansvarlige til enhver tid kan påberope seg et skjønnsmessig behandlingsgrunnlag. Det er også en viktig presisering at opplysninger ikke kan gis videre uten den registrertes samtykke.

Det er naturlig at grunnkravet til behandling av personopplysninger, som viser til de ulike vilkårene, kommer foran vilkårene. FAD støtter derfor forslaget om at en

overordnet "regibestemmelse" jf. dagens § 11 plasseres før hjemmelen om rettslig grunnlag, jf. det radikale lovutkastet § 8.

Konkrete forslag til endrede formuleringer
Vi foreslår følgende språklige endringer (endringer i *kursiv*) av formuleringen om vilkårene for å behandle personopplysninger. Vårt forslag synes å være i samsvar med JDs høringsbrev:

§ 8b 1. ledd: "Dersom vilkårene i § 8a *bokstav a-c* ikke *er oppfylt*, eller vilkåret ....." Det er vår vurdering at disse vilkårene enten er eller ikke er oppfylt. Det dreier seg ikke om vilkår man kan oppfylle gjennom ulike tiltak.

§ 8c 1. ledd: "Dersom *ingen* av vilkårene i §§ 8a *eller* 8b kan oppfylles, ..." Dette tydeliggjør at alle vilkårene i §§ 8a og 8b må vurderes og forkastes før man kan benytte et av alternativene i § 8c som grunnlag for behandling. Formuleringen i forslaget § 8c kunne ellers tolkes dit hen at det var tilstrekkelig å forkaste ett av vilkårene i §§ 8a eller 8b for deretter å finne grunnlag i § 8c, noe som neppe har vært utredernes hensikt.

Bør behandlingsansvarlige pålegges taushetsplikt?
FAD ønsker å knytte noen kommentarer til spørsmålet om den behandlingsansvarlige bør pålegges taushetsplikt for de personopplysningene som behandles i medhold av personopplysningsloven. Dette er særlig aktuelt for behandling av sensitive opplysninger. En slik taushetsplikt vil være mest nyttig for behandling av personopplysninger i privat virksomhet, da forvaltningsloven eller særlovgivning i de fleste tilfeller vil pålegge tilstrekkelig taushetsplikt i offentlig sektor.

Det kan anføres at bruk og utlevering av personopplysningene vil være begrenset av at opplysningene ikke kan benyttes til andre formål enn innsamlingsformålet uten at det foreligger klar hjemmel. Vi mener likevel at en eksplisitt taushetsplikt i personopplysningsloven vil være viktig for å tydeliggjøre at personopplysninger ikke kan utleveres til utenforstående med mindre utleveringen har rettslig grunnlag. Vi ber derfor JD vurdere en bestemmelse som pålegger den behandlingsansvarlige og alle han gir tilgang til personopplysninger, en plikt til å bevare taushet om de personopplysningene vedkommende får tilgang til. Bestemmelsen må også ledsages av en sanksjoneringsmulighet.

5. OVERFØRING AV PERSONOPPLYSNINGER TIL UTLANDET

Personvern er en global problemstilling. Etter en kraftig teknologisk utvikling, skjer det nå en stor grad av interaksjon over landegrenser. Dette innebærer behandling av personopplysninger om én stats borgere i en annen stat med andre regler for personvern. Spesielt aktuelt er dette i immigrasjonssaker, justissaker og innen samferdsel. Offentliggjøring av opplysninger på Internett er også av betydning for overføring av opplysninger til utlandet. Det er derfor viktig med lovgivning som

forhindrer misbruk av personopplysninger om norske borgere ved overføring av opplysninger til utlandet.

Utredernes mandat innebar bl.a. å vurdere om samtykke slik det er hjemlet i dagens pol. § 30 a), er tilstrekkelig unntaksgrunn fra overføringsvilkår i pol. § 29. Artikkel 29-gruppen har uttalt at medlemsstatene kan bestemme at unntaket ikke gjelder i visse tilfeller, og at unntakene uansett skal tolkes restriktivt. Det er altså mulig å unnta samtykke som grunnlag for overføring i visse tilfeller. Et spørsmål er om visse grupper på gitte vilkår bør avskjæres fra adgangen til å samtykke til overføring av personopplysninger til utlandet. FAD mener likevel at enkeltindividet mister for mye av sin handlefrihet og selvbestemmelsesrett i relasjon til utenlandske aktører dersom muligheten til å samtykke avskjæres.

Å samtykke til å overføre opplysninger til utlandet, betyr at man mister kontroll over opplysningene i større grad enn ved samtykke til nasjonal bruk. Dette gjør det også vanskeligere å trekke samtykket tilbake. Å overskue disse konsekvensene ved avgivelse av samtykke krever at den enkelte har fått tilstrekkelig informasjon om formålet med behandlingen, sikkerhetsrutiner og om regelverket i den stat opplysningene overføres til. Det bør altså stilles strenge krav til informasjonen som skal ligge til grunn for samtykke, ref. utredernes lovutkast § 30 a).

FAD støtter JDs utgangspunkt om å beholde dagens teknologinøytrale utforming av personopplysningsloven §§ 29-30. Reglene om overføring av personopplysninger til utlandet og hvordan disse skal forstås og anvendes i forbindelse med publisering på Internett, kan av pedagogiske og praktiske grunner omtales i forskriftene til personopplysningsloven. I utgangspunktet må det være de alminnelige behandlingsreglene i §§ 8 og 9 som skal legges til grunn for om en behandling er lovlig og om den eventuelt utløser meldeplikt. Ved publisering på Internett vil man uansett ikke kunne bestemme om utleveringen skjer til et land med tilfredsstillende personvernlovgivning eller et "3. land".

6. MELDE- OG KONSESJONSPLIKTEN

Personopplysningsloven inneholder en omfattende meldeplikt for behandling av personopplysninger. Mye av hensynet bak meldeplikten er at meldingene skal gi grunnlag for tilsynets kontrollvirksomhet. Dersom dette skal fungere, må meldingenes innhold være relevant, og meldingene må ha et format som gjør dem anvendelige i tilsynsvirksomheten. Det er også viktig at innholdet er oppdatert, noe som er forsøkt sikret ved at den behandlingsansvarlige har en plikt til å oppfriske meldingene hvert tredje år. Det siste overholdes tilsynelatende i liten grad. Ved revisjon av loven, bør det være et mål å finne gode og praktiske løsninger for melde- og konsesjonsreglene, som gjør at systemet tjener de hensyn som ligger bak reglene. Verken melde- eller konsesjonsplikt bør benyttes i større omfang enn nødvendig.

Konsesjonsplikt
I sitt radikale lovforslag foreslår utrederne i § 31 at det skal gjelde meldeplikt for all elektronisk behandling av personopplysninger. Dette er en endring ift dagens meldeplikt, som også omfatter manuelle personregistre som inneholder sensitive personopplysninger. §§ 33 til 33b angir så kriterier for å beslutte at en behandling skal konsesjonsreguleres. Utrederne foreslår i rapport I pkt. 9.4.7 et system der konsesjonsplikt kan baseres på konkret vurdering fra Datatilsynet basert på den personverntrussel behandlingen representerer, forskriftsbestemt konsesjonsplikt for bestemte bransjer, formål eller behandlingsmåter, eller konsesjonsplikt styrt av oppfatningen i bestemte sammenslutninger av berørte enkeltpersoner.

FAD mener det er hensiktsmessig å redusere konsesjonsplikten, samtidig som grunnkravene til behandling av personopplysninger klargjøres og strammes inn. Det kan argumenteres for at Datatilsynets behov for kontroll gjennom konsesjonsregulering reduseres når det er strengere krav til den behandlingsansvarliges egen vurdering før en behandling igangsettes. Vi er enige i at det ikke bør være en ubetinget konsesjonsplikt for all behandling av sensitive personopplysninger. Behandlinger av andre opplysninger kan også representere en betydelig personverntrussel, f.eks. ut fra antall personer det behandles personopplysninger om. En mulig løsning kan være at Datatilsynet, ut fra en vurdering av om behandlingen kan krenke tungtveiende personverninteresser, velger ut innmeldte behandlinger for konsesjonsregulering. De fleste behandlinger som kan tenkes å tilfredsstille dette vilkåret vil trolig inneholde sensitive personopplysninger, men også andre behandlinger kan omfattes av kriteriet.

Det er på den annen side usikkert om det blir tilstrekkelig forutberegnelig både for de behandlingsansvarlige og for de registrerte når Datatilsynet kan kreve konsesjonsregulering etter kriteriene i § 33. Det er viktig når planleggingen av behandlingen igangsettes at de behandlingsansvarlige har en rimelig mulighet til å innrette seg etter om en behandling bare er meldepliktig, eller om den vil utløse konsesjonsplikt.

Vi antar det også vil være viktig for tilsynsmyndigheten at vilkårene for tilsynets konsesjonsbehandling klargjøres i loven. Dette vil trolig redusere antall henvendelser med spørsmål om konsesjonsplikt og anmodning om tilsynets forhåndsuttalelse om mulig konsesjonsplikt. FAD mener § 33 derfor må oppstille flere og klare kriterier for Datatilsynets beslutning om konsesjonsregulering. Mulige avgrensningskriterier kan bl.a. være om behandlingen inneholder sensitive opplysninger med unntak av § 2 annet ledd bokstav b, om den inneholder biologisk materiale som kan knyttes til en enkeltperson, eller om det vil bli behandlet elektroniske spor (typisk i samferdsel, bank/finans og ekom-sektoren). Disse kriteriene vil kunne inngå som elementer i en vurdering av om en behandling kan krenke tungtveiende personverninteresser, men ikke nødvendigvis innebære at behandlingen *vil* krenke slike interesser.

Det virker hensiktsmessig med forskriftsregulering av konsesjonsbehandling av bestemte personopplysningsbehandlinger. Vi mener gjeldende forskriftsregulering av konsesjonsplikt bidrar med mer forutberegnelighet. Sektorene samferdsel, elektronisk kommunikasjon og finans (herunder forsikring) er typiske eksempler på sektorer der det lagres store mengder personopplysninger med et betydelig potensial for utilsiktet bruk. I tillegg er særlig samferdsel, med økende bruk av elektroniske betalingsløsninger, og ekom-sektoren, eksempler på sektorer der det i økende grad behandles personopplysninger som den registrerte mer eller mindre ubevisst legger igjen når de elektroniske alternativene brukes. Vi mener derfor disse sektorene er eksempler på områder hvor konsesjonsplikten bør reguleres i forskrifts form.

Vi er i tvil om hensiktsmessigheten av det "demokratiske elementet" som foreslås innført gjennom en rett for registrerte personer til å kreve konsesjonsbehandling. En ordning som den som foreslås i lovforslaget § 33a vil, slik vi ser det, kunne åpne for omfattende prosess. I bestemmelsen bokstav a) foreslås det at konsesjonsbehandling skal skje på grunnlag av at 40 % av de som *vil bli* registrert krever det. Ofte er det svært vanskelig å anslå hvor mange som vil bli registrert, og dermed tilsvarende vanskelig å vite hva som er 40 % av denne gruppen. Etter bokstav b kan 60 % av medlemmene i en organisasjon kreve en behandling konsesjonsbehandlet. Det fremgår ikke at behandlingen må berøre organisasjonenes medlemmer. Det er heller ikke satt krav til selve organisasjonen, dvs. selve organiseringen, antall medlemmer etc. Vi mener derfor en bestemmelse som § 33b vil bli upraktisk og vanskelig å anvende. Videre er det slik at de personvernsaker borgerne engasjerer seg i, ikke nødvendigvis er de sakene som inneholder de største personverntruslene. Det er derfor ikke gitt at "det demokratiske elementet" vil gi den effekten man kunne håpe. Vi tror imidlertid at Datatilsynet, gjennom sin mulighet til å konsesjonsbehandle i medhold av § 33, vil kunne ivareta de relevante hensynene på en god måte.

Meldeplikt

FAD er enig med utrederne i at meldesystemet bør effektiviseres slik at Datatilsynet lett kan gjøre nytte av informasjonen som meldingene inneholder. Vi er enige i at det er en god idé om bestemte typer informasjon i meldingen utløser et automatisk varsel til Datatilsynet. Det gjør det lettere for tilsynet å plukke ut meldinger de ønsker å se nærmere på, for eksempel meldinger som kan gi grunnlag for konsesjonsvurdering etter forslaget § 33. Meldeskjemaene må videre utformes slik at tilsynet får relevant informasjon for de vurderinger som skal foretas, men samtidig unngår å motta store mengder informasjon av mindre verdi. I tillegg må det tas hensyn til at et meldesystem ikke skal oppleves tyngende og uhensiktsmessig for næringslivet/de behandlingsansvarlige. Det er en utfordring å ta hensyn til de ulike interessene, og tilsynets erfaringer med dagens system vil være grunnleggende for vurdering av et nytt eller endret system.

I dag gjelder en plikt for de behandlingsansvarlige til å innlevere ny melding tre år etter forrige innmelding. På denne måten vil man kunne fange opp endringer i

behandlingene som av en eller annen grunn ikke er meldt inn. Det er sannsynlig at mange endringer i behandlinger ikke blir meldt til Datatilsynet, ofte av ren forglemmelse. Hvorvidt den behandlingsansvarlige husker å sende fornyet melding, vil være en indikasjon på hvor godt virksomheten kjenner og følger personopplysningsloven. Det fremstår likevel ikke som noe selvstendig poeng at den behandlingsansvarlige skal huske å sende ny melding til Datatilsynet etter en gitt tid. Det viktigste må være at tilsynet får den informasjonen som er nødvendig for å kunne følge opp etterlevelse av personopplysningsloven. Meldesystemet bør derfor generere en automatisk påminnelse til den behandlingsansvarige når det nærmer seg tid for ny og oppdatert melding til tilsynet.

I lovforslaget § 31 annet ledd foreslås en plikt for den behandlingsansvarlige til å informere personer som vil bli berørt av en personopplysningsbehandling. I mange tilfeller vil dette innebære en plikt til å orientere allmennheten. En positiv effekt ved en slik orienteringsplikt vil være at flere blir klar over personopplysningsbehandlinger, og at vi får mer debatt om personvern. Dette engasjementet vil være nyttig når Datatilsynet skal vurdere om enkelte behandlinger er av en slik karakter at de bør konsesjonsreguleres med hjemmel i § 33, fordi engasjementet vil bringe "det demokratiske elementet" inn i tilsynets vurdering. Den offentlige debatten om en behandling vil også kunne gi den behandlingsansvarlige nyttige korrektiv i forhold til om en behandling er fornuftig eller ikke, ref. engasjementet rundt fødselsdato i telefonkatalogen på internett for en tid siden. Denne tjenesten forsvant etter massiv kritikk fra publikum.

En mindre omfattende konsesjonsplikt vil nødvendigvis måtte ledsages av en reell mulighet for Datatilsynet til å plukke ut behandlinger blant de innmeldte behandlingene som man ønsker å se nærmere på med tanke på ev. konsesjonsbehandling. Dersom en innsendt melding fører til at Datatilsynet beslutter å konsesjonsbehandle en sak, må den behandlingsansvarlige få et varsel om dette i rimelig tid før behandlingen skal ta til. For å gi Datatilsynet rimelig tid til behandling av saken, antar FAD at meldinger ikke bør innleveres til tilsynet senere enn 45 dager før planlagt oppstart. Det må kunne legges til grunn at de fleste behandlingsansvarlige har detaljene i den planlagte behandlingen klar 45 dager før planlagt oppstart. Dette fremstår derfor etter vår vurdering ikke som en urimelig tidlig meldefrist.

Det er videre FADs vurdering at unntak fra meldeplikten, slik de fremkommer i personopplysningsforskriften kap. 7, neppe bør videreføres i det omfang fritakene har i dag. Meldeplikt er bevisstgjørende for den behandlingsansvarlige, og kan være nyttig for Datatilsynets tilsynsvirksomhet. Det kan imidlertid vurderes en forenklet meldeplikt for en del behandlinger, særlig behandlinger som antas å representere små personverntrusler, slik som mange av de behandlingene som i dag er unntatt fra meldeplikt. Den forenklede meldeplikten kan reguleres nærmere i forskrift.

Unntakene fra meldeplikten som i dag finnes i forskriften, gjelder registre og behandlinger som antas å representere liten personvernrisiko, som bl.a. kunde- og leverandørregistre mv. Unntakene gjelder et stort antall registre. FAD ser at en generell meldeplikt for disse, selv om den forenkles, vil kunne innebære en fare for "byråkratisering". Det er dessuten knyttet usikkerhet til i hvor stor grad Datatilsynet vil ha ressurser til å nyttiggjøre seg den informasjonen som innkommer. For at en utvidet meldeplikt skal føre til den positive endring som potensielt ligger i systemet, er det derfor avgjørende at tilsynet kan håndtere en slik lovendring som FAD foreslår. Det stilles også store krav til utforming av et godt elektronisk meldesystem.

7. FJERNSYNSOVERVÅKING

Innledning

Til tross for at bruken av fjernsynsovervåking har blitt stadig mer utbredt, er det lav kunnskap om og etterlevelse av reglene som regulerer dette. I henhold til Datatilsynets rapport, er de fleste klar over at det stilles krav om melding til Datatilsynet og krav om skilting i forbindelse med overvåking. Reglene blir likevel ofte brutt. Bevisstheten rundt kravene til behandlingsgrunnlag og rettslig grunnlag til behandling av personopplysninger, er lav. Dette må antas å bero mye på andre omstendigheter enn sviktende regulering. FAD mener likevel lovendringer vil være et av flere tiltak som vil bedre den manglende etterlevelsen av regelverket. Datatilsynet uttaler at reglene bør være lettfattelige, og hovedsakelig stå samlet på et sted, noe FAD i prinsippet støtter.

Utforming av personopplysningslovens kap. VII om fjernsynsovervåking

Da det ikke lå innenfor utredernes mandat å gjøre rede for behov for endringer på området for fjernsynsovervåking, er dette utelatt fra deres radikale lovforslag. Dersom store deler av det radikale lovforslaget gjennomføres, må reglene om fjernsynsovervåking tilpasses dette. Dette gjelder spesielt dagens henvisningsregel i pol. § 37, som henviser til bestemmelse som endres betydelig med det radikale lovforslaget.

Det bør fremgå av lovens saklige virkeområde at den også gjelder for kameraovervåking. For øvrig mener FAD at reguleringen av fjernsynsovervåking er mest oversiktlig dersom man opprettholder dagens struktur med et eget kapittel i personopplysningsloven.

Begrepet "fjernsynsovervåking"

Datatilsynet oppfatter begrepet "fjernsynsovervåking" som utdatert og foreslår at det erstattes med "kameraovervåking". FAD støtter Datatilsynet i at begrepet "kameraovervåking" slik det benyttes i dagligtalen i større grad samsvarer med lovens definisjon i pol. § 36 enn den allmenne forståelse av "fjernsynsovervåking". I det følgende benyttes begrepet kameraovervåking i stedet for fjernsynsovervåking.

Det kan også tenkes at definisjonen bør endres til å omfatte mer enn hva den gjør i dag. I dag er det kun bruk av "fjernbetjent eller automatisk virkende fjernsynskamera,

fotografiapparat eller lignende apparat" som omfattes. Datatilsynet mener formålet med overvåkingen må være avgjørende, slik at bruk av manuelle overvåkingsapparater også omfattes. FAD mener det foreligger gode grunner for å gi bestemmelsen en slik utvidet virkeområde, men på en måte som gjør det tydelig at det kun omfatter systematisk overvåkning med karakter av personovervåkning. FAD støtter Datatilsynet i at også bruk av slike manuelle overvåkningsinstrumenter bør omfattes. Vi foreslår følgende lovtekst;

"med *kameraovervåking* menes vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende fjernsynskamera, fotografiapparat eller lignende apparat. *Også bruk av manuelt apparat omfattes der dette bærer preg av systematisk overvåking.*"

Behandlingsgrunnlaget ved kameraovervåking

Behov for utdyping av pol. § 8 bokstav f

Datatilsynet foreslår at det gis en uttrykkelig regulering av behandlingsgrunnlag for kameraovervåkning, med en mer uttømmende angivelse av interesser som skal vernes. FAD er enig i at vilkårene i § 8 f, som ofte blir benyttet som behandlingsgrunnlag ved kameraovervåking, er vage. Det bør komme tydeligere frem at utgangspunktet er at kameraovervåking ikke skal forekomme, og at man trenger en særskilt grunn for å fravike dette. I likhet med Datatilsynet, mener FAD det vil gi større oversikt og et mer tilgjengelig regelverk dersom man unngår en henvisningsbestemmelse som dagens § 37, og det rettslige grunnlaget i stedet beskrives uttømmende i kapittelet om kameraovervåking.

Lovteksten bør utformes slik at de rettslige grunnlag retter seg direkte mot kameraovervåking. Ved angivelse av det skjønnsmessige rettsgrunnlaget, bør det klart fremgå at det skal foretas en forholdsmessighetsvurdering. Hvilke formål som kan utgjøre en berettiget interesse i å iverksette kameraovervåking; så som hensynet til liv og helse, bør angis eksplisitt. Datatilsynet uttrykker bekymring for konsekvensene av å angi kriminalitetsbekjempelse som et legalt formål for kameraovervåkning. Troen på dette som virkemiddel for å bekjempe kriminalitet, har vist seg å være langt høyere enn den reelle effekten. Vi anbefaler derfor at regelverket suppleres med en bestemmelse om at dersom kameraovervåking skal igangsettes som kriminalitetsbekjempende virkemiddel, skal tiltaket ha grunnlag i en risiko- og sårbarhetsanalyse. Resultatet av risiko- og sårbarhetsanalysen skal dokumenteres, ref. personopplysningsforskriften § 2-4 om risikovurderinger.

Kameraovervåking og sensitive personopplysninger

Normalt vil de sensitive personopplysningene man fanger opp gjennom kameraovervåking tilsvare situasjoner/opplysninger som kan observeres i det offentlige rom. Det kan derfor føre for langt å karakterisere all kameraovervåking som behandling av sensitive personopplysninger. Personvernnemndas avgjørelser, PVN-2005-12 og 13, der nemnda konkluderte med at kameraovervåking er å anse som behandling av sensitive personopplysninger, tydeliggjorde et behov for å avklare

spørsmålet om sensitivitet, spesielt fordi det etter dagens system utløser en konsesjonsplikt. Om dette er av betydning også etter lovrevisjonen, avhenger av om skillet mellom det rettslige grunnlaget for behandling av henholdsvis sensitive og "ordinære" personopplysninger oppheves i tråd med utredernes forslag. Dersom man velger å fjerne dette skillet, vil det ikke være avgjørende for konsesjonsplikten om kameraovervåking anses som behandling av sensitive personopplysninger. Dersom det innføres et system der det er opp til Datatilsynet å avgjøre om konsesjon skal pålegges, vil imidlertid sondringen mellom sensitive og "ordinære" opplysninger likevel kunne få betydning for innholdet i meldingen til Datatilsynet. JDs forslag er at kameraovervåking som hovedregel skal regnes som behandling av sensitive personopplysninger (se mer om dette nedenfor). Hvis en slik regel innføres, bør det fremgå av den innsendte meldingen dersom kameraovervåkingen *ikke* tar sikte på å avdekke sensitive personopplysninger. Dette vil kunne få betydning for Datatilsynets vurdering av om behandlingen skal underlegges konsesjonsplikt.

Det bør være formålet med behandlingen som avgjør om kameraovervåkingen skal anses som behandling av sensitive personopplysninger. Dersom overvåkingen tar sikte på å avdekke sensitive personopplysninger, bør den reguleres deretter. Dette nødvendiggjør et forhåndsdefinert formål med overvåkningen, noe som kan fungere bevisstgjørende for den behandlingsansvarlige. Kameraovervåking bør ikke karakteriseres som behandling av sensitive personopplysninger som følge av at opptak tilfeldigvis avdekker sensitive opplysninger. Det er grunn til å regulere dette uttrykkelig i det nye kapittelet om kameraovervåking.

Svært mye kameraovervåking gjennomføres for å forhindre eller avdekke straffbare forhold. Når formålet er utslagsgivende for om behandlingen karakteriseres som sensitiv, vil overvåkingen som en hovedregel anses som behandling av sensitive personopplysninger. Vi støtter derfor JDs forslag om en hovedregel om at kameraovervåking innebærer behandling av sensitive personopplysninger. Det bør i tillegg fremgå at dersom formålet ikke er å avdekke sensitive personopplysninger, innebærer kameraovervåkingen heller ikke behandling av sensitive personopplysninger. Det vil således gå frem av loven hva den reelle hovedregelen er, samtidig som det fremgår at formålet med overvåkingen er avgjørende for spørsmålet om sensitivitet.

Opplysninger om straffbare handlinger

Ofte vil kameraovervåking ha til formål å avdekke straffbare forhold. Dette faller ikke naturlig inn under ordlyden i pol. § 2 nr. 8 b). JD uttaler at den må forstås og tolkes slik at opplysninger om straffbare handlinger – ikke kun opplysninger om en ev. strafferettslig forfølgning, er omfattet. I denne forbindelse foreslås det å erstatte dagens formulering med "som har som formål å forhindre eller avdekke straffbare handlinger". FAD støtter at definisjonen av sensitive personopplysninger endres i tråd med dette.

Kameraovervåking vil i stor grad ha som formål å fange opp kriminell virksomhet, og vil ut fra dette ofte bli å regne som behandling av sensitive personopplysninger.

Betydningen av dette er avhengig av hvorvidt konsesjonsplikten fortsatt skal knyttes opp mot sondringen mellom sensitive og "ordinære" personopplysninger. Dersom dette skillet fortsatt skal være avgjørende, vil det være ønskelig å innta et unntak fra konsesjonsplikten for kameraovervåking.

Kameraovervåking på sted hvor en begrenset krets av personer ferdes jevnlig
Datatilsynet mener kameraovervåking bør begrenses på flere steder enn der "en begrenset krets av personer ferdes jevnlig". FAD er enig i at det er flere steder kameraovervåking er tilsvarende eller mer inngripende enn steder der en begrenset krets ferdes jevnlig. Visse steder har man en høyere forventning om ikke å bli overvåket, f.eks. på stranden eller i friluftsarealer, slik som nevnt i høringsnotatet. FAD foreslår at § 38 endres til "sted hvor en begrenset krets av personer ferdes jevnlig *eller på sted der det er rimelig å forvente at man ikke vil bli overvåket*".

Av Datatilsynets utredning s. 27 fremgår det at de mener kravet om "særskilt behov" i § 38 bør konkretiseres. Ordlyden i seg selv tilsier at forholdsmessighetsvurderingen skal være strengere enn vanlig her, men gir ingen anvisning på hvor mye som skal til eller hvilke hensyn som gjør seg gjeldende. Det kan være hensiktsmessig å spesifisere hvilke formål som i slike tilfeller vil kunne utgjøre et "særskilt behov".

Vi er enig i at bestemmelsens overskrift er misvisende i forhold til dens innhold. Denne bør etter vår mening endres til *"særskilte krav til overvåking av visse områder"*.

Varsel om kameraovervåking
Datatilsynet mener at skilting av kameraovervåking bør angi hva slags kameraovervåking det er snakk om, i tillegg til å gå angi at overvåkning skjer og hvem som er behandlingsansvarlig. Tilsynet foreslår at en lampe skal indikere når opptak foretas. Det foreslås å bruke standardsymboler for å indikere om det skjer lydopptak, ansiktsgjenkjenning osv. FAD mener imidlertid dette vil ha lite for seg, da de færreste vil vite hva symbolene betyr. Vi mener dagens regler gir et tilfredsstillende grunnlag for varsling. Det er viktigere å gjennomføre tiltak for å oppnå en bedre etterlevelse varslingsreglene enn å pålegge nye plikter.

Skillet mellom kameraovervåking med og uten bildeopptak
FAD mener det skaper unødige fortolkningsvansker når loven opererer med et utdatert skille mellom monitorering og billedopptak. I dag skjer kameraovervåking hovedsakelig digitalt, slik at opptak skjer automatisk. I den grad det foretas monitorering uten opptak, bør dette i stedet komme inn som moment i proporsjonalitetsvurderingen. Lovens virkeområde bør etter vår mening utvides til å omfatte all form for kameraovervåking. For å unngå at regulering av virkeområde spres i flere bestemmelser, bør presiseringen inntas i § 3 som regulerer lovens saklige virkeområde i stedet for i kapittelet om kameraovervåking.

Et alternativ kan være å innta en tilsvarende presisering som i dansk rett i § 3 tredje ledd: "loven gjelder for enhver form for behandling av personopplysinger i forbindelse

med kameraovervåking". Det kan være noe tvilsomt om monitorering uten opptak vil falle innenfor begrepet "behandling av personopplysninger". For å unngå tolkningstvil vil det etter FADs mening være bedre med følgende formulering: *loven gjelder for enhver form for kameraovervåking*

Et tilgrensende spørsmål, er når kameraovervåking blir å regne som behandling av personopplysning; ved opptak eller avspilling av opptaket. Personvernnemnda har i flere saker konkludert med at kameraovervåking ikke er å anse som behandling før opptaket spilles av. FAD mener dette kan medføre et unødvendig komplisert system. Vi oppfatter behandlingen som påbegynt allerede på opptakstidspunktet. Dette er også i tråd med at skillet mellom monitorering og opptak fjernes. Vi viser i tillegg til våre merknader vedrørende kravet om identifikasjon i kap. 1.

Melde og konsesjonsplikt for kameraovervåking
Underrapporterting av kameraovervåking har vist seg som et gjennomgående problem. Datatilsynet foreslår at kameraovervåking underlegges en særskilt meldeordning, eventuelt at dette registreres i andre offentlige registre. Etter dagens ordning finnes det ingen totaloversikt over kameraovervåking. FAD forutsetter at dagens meldesystem vil bli revidert, slik at et fremtidig system fungerer bedre enn dagens. Det er viktig at et slikt system legger til rette for oppfyllelse av meldeplikten for den behandlingsansvarlige, slik at systemet blir enkelt å bruke. Under forutsetning av at dagens generelle meldesystem utbygges, mener FAD melding om kameraovervåking bør ligge innenfor dette systemet. I kombinasjon med et bevisstgjørende arbeid, vil dette kunne gi bedre etterlevelse av meldeplikten.

Behandlingsansvarlige kan lett oppfatte manglende tilbakemelding på innmeldt kameraovervåking som en godkjenning av tiltaket. Det kan spørres om hensikten med meldeplikten da oppnås. Datatilsynet ønsker som hovedregel å ikke ha krav om konsesjonsplikt, men mener det bør vurderes om de kan beslutte at konkrete tilfeller av kameraovervåking, eller spesielle former for kameraovervåking, skal være konsesjonspliktige. Da ordningen med meldeplikt har båret preg av manglende etterlevelse, mener FAD det er bedre å innføre konsesjonsplikt bare for visse typer kameraovervåking. Dersom det innføres en begrenset konsesjonsplikt for kameraovervåking, bør dette reguleres i den nye loven, og det bør skje en konkret angivelse av hvilke tilfeller konsesjon er nødvendig. En ordning der det overlates til Datatilsynet å avgjøre konsesjonsplikten i enkelttilfeller, vil kunne fremstå som lite forutberegnelig. I tillegg vil reglene bli mer tilgjengelige dersom det fremgår av loven hva som er konsesjonspliktig overvåking. Dette er i samsvar med våre generelle merknader til konsesjonsplikten under kap. **Feil! Fant ikke referansekilden.**.

Datatilsynet ønsker å redusere konsesjonsbehandling, da dette etter deres oppfatning er en lite hensiktsmessig bruk av ressursene. Det kan imidlertid settes spørsmålstegn ved om dette også gjelder kameraovervåking, der overholdelsen av meldeplikten har vært lav. Utrederne uttaler at et svakt eller ikke- fungerende meldesystem, bør gjøre det mindre aktuelt å redusere omfanget av konsesjonsplikten. I tråd med dette er det mer

aktuelt å utvide konsesjonsplikten der meldesystemet har vist seg å fungere dårlig. På mange områder vil i tillegg den som ønsker å sette i verk kameraovervåking, ha så sterke interesser i overvåkningen at han ikke evner å foreta en objektiv forholdsmessighetsvurdering, slik at personvernhensyn blir nedprioritert. Å innføre konsesjonsplikt for kameraovervåking innen risikosektorer, vil sørge for en mer reell avveining mellom formålet med kameraovervåkingen og personvernhensyn. Et eksempel på et område som kan egne seg for konsesjonsregulering er kameraovervåking på skole eller i ulike typer boinstitusjoner.

8. MINDREÅRIGES PERSONVERN

Behov for lovendring

JD ber om høringsinstansenes syn på om det bør gis særregler om mindreårige i personopplysningsloven. FAD mener helt klart at det på mange områder er ønskelig med særregler for bruk av personopplysninger om barn. I Norge har vi allerede på mange områder særregler både for behandling av personopplysninger om barn og om barns (rettslige) handleevne. Regler i særlovgivning om behandling av personopplysninger vil gå foran generelle regler i personopplysningsregelverket. I tillegg eksisterer en del retningslinjer om behandling av personopplysninger om mindreårige. Noen situasjoner kan imidlertid falle utenfor gjeldende regelverk. Disse tilfellene kan det være hensiktsmessig å regulere i eller i medhold av personopplysningsloven.

Vi mener at de retningslinjer som eksisterer i dag, ikke gir samme grad av rettssikkerhet og forutberegnelighet som lovregulering på området vil gjøre. Vi er positive til at bruken av det skjønnsmessige rettslige grunnlaget i dagens § 8f reduseres for behandling av personopplysninger om barn, gjennom en endring av nødvendighetshjemmelen. Vår oppfatning er i tråd med det radikale lovforslaget, som innebærer en endring slik at opplysninger om barn under 12 år ikke skal kunne behandles med hjemmel i nødvendighetskravet. Etter vår mening vil det være bedre med en regel som gjør unntak for all behandling av personopplysninger om barn under 12 år, ikke bare der det *"i overveiende grad"* behandles opplysninger om barn under 12 år, slik det er formulert i utkastet § 8c bokstav c. Vårt forslag vil blant annet kunne forhindre behandling av opplysninger om barn for kommersielle formål.

Samtykke

Etter utredernes lovendringsforslag, vil samtykke fra den registrerte få en mer sentral betydning. I hvilken grad mindreårige har medbestemmelsesrett eller selvbestemmelsesrett i samtykkespørsmålet, er uklart i dag. Det spesielle med barns situasjon, er at retten til å bestemme over barnet skal deles mellom barnet selv og den som har foreldreansvar for barnet. Barnet får en gradvis større rett til å opptre selvstendig. Utfordringer knyttet til barnets samtykkekompetanse ligger både i forholdet til foreldrene, og utad i forhold til tredjeparter som for eksempel skole og en virtuell "virkelighet".

I helsesektoren reguleres allerede i dag barns rett til med-/selvbestemmelse. Barn over 16 år har rett til å ta beslutninger om egen helse uten at de foresatte informeres om dette. Helseopplysninger om barn mellom 12 og 16 år skal ikke gis foreldrene eller andre med foreldreansvar når barnet av grunner som bør respekteres, ikke ønsker dette, jf. pasientrettighetsloven §§ 3-4 og 4-4. Dette vil fungere som spesiallovgivning i forhold til den foreslåtte endringen i personopplysningsloven, og i henhold til lex spesialis-prinsippet gå foran denne. For å lette praktiseringen av personopplysningslovens bestemmelser i situasjoner der den registrerte er mindreårig, er det likevel ønskelig med en regulering av i hvilken grad barn generelt har rett til å bestemme over egne opplysninger.

Barns evne til å utøve rettigheter etter pol
JD oppfordrer høringsinstansene til å ta stilling til hvorvidt en eventuell særbestemmelse om barnets rett til å bestemme over egne opplysninger, bør knyttes til begrepet "*registrert person*". FAD er enig i at man bør gi en generell regulering av mindreåriges evne til å opptre som registrert person. Vi mener dette bedre kan gjøres ved å benytte en formulering som går ut på at "personer under 18 år kan *utøve rettigheter* etter bestemmelsene..."

Utrederne mener at lovregulering av barns rett til å utøve rettigheter etter loven, må ha et "innhold som harmonerer med annen eksisterende lovgivning om barn og ungdoms handleevne". Det foreslås på denne bakgrunn en grense på 15 år for at barn skal kunne opptre uten foreldrenes medvirkning. Dette samsvarer godt med for eksempel barns rett til å ta arbeid etter arbeidsmiljøloven § 11-1, barns rett til å bestemme over egne penger, jf. vergemålsloven § 33, barns rett til å melde seg inn eller ut av trossamfunn, jf. trudomssamfunnslova § 6, eller barns rett til eget skolevalg, jf. barnelova § 32. Det er videre i tråd med den grense Datatilsynet og Forbrukerombudet trakk opp i veilederen "Barn og unges personopplysninger: Retningslinjer for innhenting og bruk".

Barnets rettigheter vurderes ut fra alder og modenhet
I henhold til barneloven § 31 skal barnet få gradvis større medbestemmelsesrett. Foreldrene skal i henhold til denne bestemmelsen legge vekt på barnets synspunkt ut fra "kor gammalt og modent barnet er". Det er altså ikke utelukkende alder som er avgjørende for barnets rett til å være med på å ta avgjørelser, men også dets modenhet. Det avgjørende må være barnets evne til å forstå konsekvensene av beslutningen. Av utkastets § 6 siste ledd går det frem at foreldrene kan gripe inn i større grad enn det som følger av bestemmelsens første ledd dersom dette er nødvendig for å ivareta foreldreansvaret, altså dersom dette er til barnets beste, jf. barnelova § 30. Forslaget gir ikke rom for tilsvarende fleksibilitet når det gjelder barnets rett til selvbestemmelse tidligere enn de lovfestede alderskravene. Vi foreslår at det i tillegg inntas en presisering av at barnet kan få større grad av selvbestemmelse dersom det er klart at barnet ut fra sin modenhet fullt ut evner å forstå konsekvensene av samtykke. Vi ber JD vurdere å legge ordlyden i § 6a så nært opp til det som følger av barnelova § 31 som mulig.

Krenkelser foretatt av barnets foreldre

I tillegg til samtykkeproblematikken, ligger det en stor utfordring i at krenkelser av mindreåriges personvern nettopp kan forårsakes av barnets foreldre. Typisk eksempel er publisering av tekst og bilder av barn på internett, for eksempel i foreldrenes kamp mot myndighetene i saker om f.eks. omsorgsovertakelse. Det hjelper lite at barnet får en sterkere rett til medbestemmelse, dersom foreldrene offentliggjør opplysninger som kan skade barnet. JD reiser spørsmål om foreldres samtykkekompetanse bør underlegges særskilte begrensninger i typiske tilfeller der foreldrene representerer en risiko for barnets personvern. JD henviser til ny strl. § 390 som, i henhold til Ot.prp. nr. 22 (2008-2009), kan brukes hvis foreldre legger ut sensitiv informasjon om sine barn på Internett. Reaksjoner mot slik adferd, vil etter FADs syn være et steg på veien for å forhindre at foreldre krenker sine barns personvern på denne måten.

Samtidig mener vi at en henvisning til å benytte straffelovens bestemmelser i etterkant av en krenkelse, ikke vil være tilstrekkelige. JD viser til teorien som gir klart uttrykk for at foreldrenes rett til å samtykke på vegne av barnet, er begrenset ut fra barnekonvensjonen art. 16 og barneloven § 30 ut fra hva som er barnets beste. Det gis også uttrykk for at det i teorien er antatt at barnet kan ha større selvbestemmelsesrett til å nekte enn til å gi samtykke til inngrep eller tiltak. Dette gir etter vår mening barnet en vag beskyttelse og vil i praksis ikke gi noen beskyttelse mot foreldres feilaktige beslutninger, og dessuten ikke fungere tilstrekkelig som inngrepshjemmel for Datatilsynet i enkelttilfeller der foreldre har offentliggjort informasjon om mindreårige som burde vært holdt tilbake. FAD mener derfor det bør inntas en særskilt regulering som begrenser foreldres rett til å offentliggjøre informasjon om sine barn. Ved utformingen av en slik ny regel, vil man måtte se hen til de grunnprinsipper som kommer til uttrykk i barnekonvensjonen og barneloven. Regelen bør gi uttrykk for at barnets beste skal stå i fokus, og videreføre prinsippet slått fast i juridisk teori om at barnet har en større rett til negativ selvbestemmelsesrett, altså å nekte offentliggjøring, enn til å gi sitt samtykke til dette. Dette vil gi Datatilsynet større rom for inngrep der en krenkelse har skjedd, og vil kunne gi en viktig signaleffekt om at foreldre i større grad må respektere barnets ønsker i slike tilfeller. Videre vil det kunne skape en større refleksjon som gir grunnlag for en mer kritisk tenkning rundt spørsmål om offentliggjøring. En slik regel vil kunne bidra til at barn ikke uforvarende havner i situasjoner det må ryddes opp i i ettertid.

Innsyn i informasjon

Hva gjelder innsyn i informasjon om barnet, er vi enig i at det bør inntas et unntak fra den registrertes rett til selv å få innsyn i opplysninger, fordi, som utrederne foreslår i rapport I s. 147, "vedkommende på grunn av ung alder eller andre forhold har utilstrekkelig evne til å forholde seg til opplysningene". Selv om det ikke er tilrådelig at barnet selv får innsyn i opplysninger, skal opplysninger gjøres tilgjengelig for en representant for barnet, hvilket sikrer et minimum av innsyn.

9. PERSONVERNOMBUD

Innledning

Utrederne foreslår å lovfeste personvernombudsordningen, samt å detaljregulere ordningen i større grad enn i dag. Datatilsynet har satset betydelige ressurser på personvernombud (PVO) de senere årene. Mange offentlige etater og private virksomheter har i dag PVO. Det er imidlertid ikke på noe tidspunkt gjennomført en grundig evaluering av ordningen. FAD ga i RNB 2009 Datatilsynet midler til et prosjekt om personvernombudsordningen som skal innbefatte en evaluering av ordningen. Prosjektet skal gå over to år, og ferdigstilles medio 2011. Vi mener denne evalueringen er viktig før man vurderer endringer til en mer omfattende ordning enn den vi har i dag. Vi er likevel enige med utrederne i at i den grad ordningen skal videreføres, bør den lovfestes.

Det er FADs erfaring at opprettelse av PVO i en virksomhet ikke nødvendigvis er en garanti for at den behandlingsansvarlige ivaretar sine plikter etter personopplysningsloven på en tilfredsstillende måte. Opprettelse av PVO ser, tvert i mot, i noen tilfeller ut til å fungere som en sovepute. Utrederne synes å ha gjort noen av de samme observasjoner, ref. merknader under rapport I pkt. 10.2. Når dette er sagt, bør det selvsagt presiseres at mange PVOer gjør en god jobb, er en ressurs både for den behandlingsansvarlige og de registrerte, og ivaretar sine oppgaver på en utmerket måte.

De nedenstående merknadene er gitt ut fra den forutsetning at JD velger å lovfeste og videreføre dagens ordning med personvernombud. Merknadene er imidlertid ikke et uttrykk for at FAD ønsker utvidelser av ordningen før den har vært gjenstand for en grundig evaluering.

Begrepet "personvernombud"

For så vidt gjelder begrepet "personvernombud", er vi enige med JD i at dette ikke er et heldig begrep. *Ombud* i Norge forbindes med noe annet enn det som ligger i personvernombudsordningen. Derimot tror vi ordningen kan være tjent med begrepet "personopplysningsrådgiver". Dette er et begrep som kan åpne for at vedkommende er rådgiver både for den behandlingsansvarlige og de registrerte i spørsmål som angår behandling av personopplysninger. Samtidig avgrenser begrepet mot at vedkommende er rådgiver for alt som kan ha med personvern å gjøre, da personvern er mye videre enn personopplysningsvern. Begrepet *personvernansvarlig*, som lanseres av utrederne som et mulig alternativ, vil etter vår vurdering kunne virke villedende, da vedkommende ikke vil være *ansvarlig*. Ansvaret vil ligge hos den behandlingsansvarlige uansett om det er oppnevnt PVO eller ikke. Det er derfor viktig å velge et begrep som ikke gir inntrykk av at PVOen har større ansvar og myndighet enn vedkommende faktisk har. Dette bør fremgå klart av loven.

Interne vs. eksterne ombud
I dag har noen virksomheter PVOer som er rekruttert internt, mens noen har ombud som ikke er ansatt i virksomheten (eksternt ombud). Regelverket åpner for begge deler, og begge deler har sine fordeler og ulemper. Et internt ombud vil lettere se og forstå utfordringer det bør arbeides med, og ofte være mer tilgjengelig for alle parter enn et eksternt ombud. Et eksternt ombud derimot, vil trolig kunne føle seg friere til å påpeke forhold som bør rettes opp enn et internt ombud. Vi deler JDs vurdering om at ombudet primært skal bistå den behandlingsansvarlige i å etterleve regelverket, og mener at dette trolig best kan ivaretas av en person som befinner seg i virksomheten. Dersom JD velger å fremme forslag om at PVO skal være internt ansatt, bør det likevel presiseres at det er fullt mulig å benytte eksterne rådgivere, men at disse ikke vil falle inn under den lovfestede ordningen.

Når det gjelder utredernes forslag om å kombinere en ordning med interne PVOer med eksterne personvernrådgivere/personvernkontorer, er dette selvsagt ikke utelukket. Mange advokatfirmaer tilbyr for eksempel bistand på personvernområdet, og kan sånn sett fungere som eksterne personvernrådgivere. Men FAD er skeptisk til å institusjonalisere denne bistanden på en måte som innebærer opprettelse av offentlig finansierte bistandstjenester på siden av Datatilsynet, slik utrederne kan synes å åpne for i rapport I pkt. 10.4.5.

Personvernombudets oppgaver og plikter
Det er viktig å avklare PVOens oppgaver og plikter. Det må for det første være åpenbart at PVO ikke har noe rettslig ansvar for den behandlingsansvarliges etterlevelse av personopplysningsloven. Vedkommende skal bistå den behandlingsansvarlige i å oppfylle sine plikter etter personopplysningsloven, og kan f eks bistå med konkrete tilpasninger i virksomheten slik at den blir i samsvar med kravene.

I sitt forslag til bestemmelser om personvernombudsordningen, har utrederne foreslått en bestemmelse som skal regulere ombudets oppgaver. Bestemmelsen er tredelt, basert på hvem som skal motta bistand. Disse er de registrerte, den behandlingsansvarlige og de ansatte hos den behandlingsansvarlige. Etter FADs vurdering er det bedre å fokusere på hvilke oppgaver ombudet skal utføre, snarere enn å ha fokus på hvem de utføres for. Dersom PVOens oppgaver skal regelfestes, mener vi listen over sentrale PVO-oppgaver som Datatilsynet har på sine nettsider, i hovedtrekk kan videreføres. Regelfestingen bør i så fall skje ved at det gis hjemmel til å fastsette nærmere forskrifter om PVOenes oppgaver. Det bør videre vurderes plikt for PVOen til å rapportere brudd på regelverket til Datatilsynet, dersom den behandlingsansvarlige ikke viser vilje eller evne til å rette forholdet.

FAD støtter imidlertid utrederne i at det ikke bør være PVOens oppgave å føre fortegnelse over behandlinger av personopplysninger. Dersom det skal føres en slik fortegnelse, bør informasjonen finnes hos Datatilsynet, og ikke bare hos PVOen. Vi stiller samtidig spørsmål ved om det bør innføres en plikt for PVOen til å ha et arkiv over egen korrespondanse. Et slikt arkiv vil kunne være nyttig f.eks. for Datatilsynet

ved tilsyn hos den behandlingsansvarlige. Jo mer formalisert en ordning med PVO er, jo strengere krav må kunne stilles til deres arbeid og dokumentasjon av dette.

Betydningen av å opprette personvernombud
Utrederne foreslår lettelser for den behandlingsansvarlige ved opprettelse av PVO. Blant annet foreslås det redusert dokumentasjonsplikt for informasjonssikkerhet og internkontroll. Det antydes at PVO kan erstatte internkontroll. FAD mener dette kan få flere uheldige konsekvenser. Et internkontrollsystem skal dokumentere hvorledes den behandlingsansvarlige etterlever sine plikter etter personopplysningsloven. Et slikt system vil være nyttig for en PVO når denne skal ivareta sine oppgaver, ikke minst hos store behandlingsansvarlige eller for eksterne PVOer. Å la PVO erstatte dokumentasjonsplikten vil neppe ha en positiv effekt for personvernet, og er derfor etter vår vurdering ikke heldig.

FAD stiller seg tvilende til om det er behov for regler om stillingsvern for PVOen, slik dette er omtalt i høringsnotatet pkt. 9.3.5.1. Vi kan heller ikke se at det er behov for regler om ombudets forhold til Datatilsynet. FAD mener at ombudet, uten annen særskilt hjemmel, ikke vil være underlagt tilsynets styrings- eller instruksjonsmyndighet på annen måte enn det den behandlingsansvarlige vil være. Vi kan derfor ikke se at det er behov for regler som regulerer dette.

For så vidt gjelder opphør av PVO i en virksomhet, er det neppe behov for å regulere virksomhetens egen mulighet til å avvikle ordningen. Det fremstår derimot som hensiktsmessig å innføre regler om i hvilke situasjoner Datatilsynet kan eller skal trekke tilbake en godkjenning av et ombud. Dersom ordningen er noe som markedsføres som et "kvalitetsstempel", er det avgjørende at publikum kan ha tillitt til at ordningen faktisk fungerer. Dersom det å ha PVO skal kunne oppfattes som et tegn på at personvern tas på alvor, må også ombud som ikke utfører sine oppgaver i samsvar med regelverket fjernes. Det bør derfor fremgå av regelverket hva som kan eller skal gi grunnlag for å kalle tilbake en godkjenning av et PVO.

Det fremgår av det ovenstående at FAD i hovedsak mener det er flere sider knyttet til PVOs virksomhet, ansvar og rolle som det er nødvendig å få bedre innsikt i effekten av før man detaljregulerer dette temaet. Vi mener derfor det i dag ikke bør gjøres mer enn ev. å lovfeste en klar hjemmel i personopplysningsloven til å gi nærmere regler om PVOs ansvar, rettigheter og ordningens betydning for andre regler.

10. ANDRE PROBLEMSTILLINGER

Personopplysningsloven og særlovgivningen
I utgangspunktet ber ikke Justisdepartementet om høringsinstansenes uttalelse om forholdet mellom pol og særlovgivningen utover forslaget om å ta inn en bestemmelse som klargjør forholdet til taushetsplikt.

FAD vil likevel fremheve viktigheten av å se særlovgivningen i sammenheng med aktuelle endringsforslag i personopplysningsloven. Da personopplysningsloven ble utformet var det viktig at flere av de tidligere innarbeidede begreper fra "personregisterloven" ble videreført. Bruk av innarbeidede begreper er både pedagogisk og rettsikkerhetsmessig gunstig. Vi mener endringer i loven bør være begrunnet i ev. manglende samsvar mellom norske rettsregler og direktivet, samt ev. ut fra behovet for å endre uheldig eller utilsiktet praktisering av regelverket.

Det er også viktig å ta hensyn til at f.eks. helsesektoren har måttet forholde seg til nye og meget omfattende lovverk i løpet av det siste tiåret. I sektorer med "rettsanvendere" som i utgangspunktet har liten tradisjon for å anvende regelverk bør det utvises varsomhet med å anbefale omfattende "regelverksdugnader". Derimot bifaller FAD at det arbeides for å sikre at det henvises til personopplysningsloven fra annet relevant lovverk. Vi mener det er riktig å ta med en henvisning til bestemmelser om taushetsplikt, og at utredernes forslag er hensiktsmessig.

Personopplysningslovens struktur
Utrederne har laget et hensiktsmessig skille mellom a) strukturen i loven selv og b) forholdet mellom loven og forskriften.

a) Intern struktur
Vi er enige med utrederne i at en omplassering av bestemmelsene vil gi en mer kronologisk korrekt struktur i kapittel II. Vi er derimot ikke enige i forslaget til oppdelingen av § 8, se vår omtale i kap. 4, under punktet om nødvendighetsgrunner. I forbindelse med denne lovendringen er det viktig å utarbeide gode veiledninger til ulike grupper av både regelanvendere og de registrerte. Ikke minst er det viktig med godt veiledningsmateriell om den registrertes rettigheter. Lov som sådan har i liten grad tradisjon for å være spesielt godt egnet som allmenn informasjon.

b) Struktur knyttet til sammenheng mellom personopplysningsloven og forskriften
Utrederne påpeker at enkelte av bestemmelsene som er gitt i forskrift bør tas inn i selv loven på grunn av at bestemmelsene etter sitt innhold tilhører lovnivå og ikke forskriftsnivå. På bakgrunn av dette støtter FAD utredernes standpunkt om å flytte følgende bestemmelser fra personopplysningsforskriften til personopplysningsloven:

- pof § 1-3 om saklig virkeområde
- pof §§ 2-1 om sikring av personopplysninger
- pof § 10-1 om Personvernnemndas kompetanse

FAD støtter ikke forslaget om å flytte dagens forskriftsbestemmelse om forbud mot fødselsnummer utenpå brevsending til loven. FAD mener i utgangspunktet at bestemmelsen burde være unødvendig. For det første er den med på å opprettholde myten om at fødselsnummer er en hemmelig opplysning, for det andre er det neppe noe stort problem i praksis i dag at fødselsnummer blir trykket utenpå

konvolutt/brevsending. Dessuten vil en synliggjøring av fødselsnummer utenpå postsending kunne innebære at den behandlingsansvarlige urettmessig utleverer personopplysninger til utenforstående, og bør i så fall behandles på samme måte som all annen urettmessig utlevering til utenforstående. En endring av ordlyden slik det foreslås vil dessuten innebære at alle e-postmeldinger som inneholder fødselsnummer vil måtte krypteres, noe som vel ikke er hensikten med endringen. Den teknologiske virkeligheten i dag gjør det praktisk talt umulig å etterleve en slik bestemmelse.

Forholdet mellom personopplysningsloven og personopplysningsforskriften
FAD deler JDs vurdering av at reglene om kredittopplysningsvirksomhet, som i dag finnes i personopplysningsforskriften kap. 4, bør gjennomgås med tanke på revisjon så snart som mulig. Allerede ved Stortingets vedtakelse av personopplysningsloven ble det forutsatt at særskilt regulering av kredittopplysningsvirksomhet skulle vurderes. I Innst. O. nr. 51 (1999-2000), pkt. 7 fremgår det at "...komiteen forutsetter at det igangsettes et arbeid for at de særregler som bør gis for kredittopplysningsvirksomhet gis i lovs form.".

FAD mener at det ikke er forhold ved kredittopplysningsvirksomhet som tilsier at det ikke fremdeles er grunn til å lovregulere virksomheten. FAD mener derfor at kredittopplysningsvirksomhet bør reguleres i særlov så snart som mulig. Særlovsregulering av kredittopplysningsvirksomhet er for eksempel tilfellet i Sverige, der Datainspektionen har ansvaret for å forvalte kreditupplysningslagen (1973:1173) i tillegg til personuppgiftslagen (1998:204). Etter det vi kjenner til, fungere dette godt.

Ved å regulere kredittopplysningsvirksomhet i særlov, vil man bl.a. unngå de uklarheter som i dag kan oppstå ved at personopplysningsloven i utgangspunktet kun gjelder for behandling av opplysninger om fysiske personer, men at bestemmelsene om kredittopplysning likevel gjelder både juridiske og fysiske personer.

Informasjonssikkerhet og internkontroll
Personopplysningslovens regler om informasjonssikkerhet og internkontroll oppfattes av mange behandlingsansvarlige som vanskelige. Dette er dokumentert gjennom ulike undersøkelser. FAD ser derfor positivt på at JD i sitt høringsnotat har tatt fatt i noen utfordringer knyttet til disse bestemmelsene i håp om å få til klargjøringer.

For så vidt gjelder reglene om internkontroll/vedlikehold av systematiske tiltak som skal sikre etterlevelse av lovens regler, tror vi det vil ha en positiv effekt å konkretisere kravene til innholdet i slike systemer direkte i loven. På denne måten blir det trolig enklere for den behandlingsansvarlige å etablere et internkontrollsystem. FAD støtter derfor JDs forslag til konkretisering av innholdet i internkontrollsystemet direkte i loven.

JD åpner i høringsnotatet for å endre innholdet i informasjonssikkerhetsbestemmelsen i nåværende § 13. FAD er i tvil om en endring slik at informasjonssikkerheten eksplisitt

skal omfatte opplysnings*kvalitet*, vil medføre realitetsendring. Etter personopplysningsloven § 11 har den behandlingsansvarlige plikt til å sørge for at de opplysningene som behandles er av god kvalitet i forhold til formålet. Internkontrollen skal etter gjeldende § 14 omfatte systemer for å sikre denne kvaliteten. Informasjonssikkerheten skal omfatte tiltak for å sikre opplysningenes integritet, dvs. at de ikke kan endres av uautoriserte eller uten at det er villet. Gjennom tiltak for å sikre opplysningenes integritet, vil man ivareta opplysningenes kvalitet. Informasjonssikkerheten kan, etter vår vurdering, derigjennom sies å omfatte opplysningskvaliteten. Opplysningene skal være av god kvalitet, og de skal ikke kunne endres uautorisert, noe som sikrer at den gode kvaliteten vedvarer. Vi kan etter dette ikke se at det er nødvendig å endre gjeldende § 13 på dette punktet.

Databehandlerens rådighet over personopplysninger
Pol § 15, omhandler databehandlerens rådighet over personopplysninger. Bestemmelsen viser til at rådigheten, herunder begrensninger i denne, skal fremgå av avtale. Avtalen består mellom den behandlingsansvarlige og databehandleren. Den samme avtalen er også bestemmende for databehandlers mulighet til å overlate opplysningene til andre for lagring eller bearbeidelse.

FAD foreslår at det i pol § 15 inntas en forskriftshjemmel som åpner for å gi nærmere bestemmelser om hovedinnholdet i den avtalen som skal inngås mellom den behandlingsansvarlige og databehandleren. Dette vil bidra til å gi større forutberegnelighet for behandlingsansvarlig, databehandler og de registrerte.

Automatiserte avgjørelser
JD viser til pol § 22 og stiller spørsmål ved om det er ønskelig at de registrerte skal gis mulighet til å få overprøvet helautomatiske avgjørelser. FAD antar dette i så fall må dreie seg om en annen type overprøving enn det som følger av § 25. Vi støtter i så fall en slik utvidet overprøvingsmulighet.

Straffebestemmelsen i personopplysningsloven § 48
Overtredelse av personopplysingslovens bestemmelser må utvilsomt være forbundet med straffesanksjonering for å kunne fungere effektivt. Det er imidlertid en forutsetning at straffesubjektet fremgår på en tydelig måte. Utrederne mener at pol. § 48 slik den lyder i dag, ikke i tilstrekkelig grad klargjør hvem som rammes av straffeansvaret. JD mener derimot det også etter dagens utforming går frem at det er den behandlingsansvarlige som er straffeansvarlig, da det er behandlingsansvarlig som er pliktsubjekt etter de konkrete bestemmelsene det vises til i § 48. Selv om den behandlingsansvarlige kan delegere arbeidsoppgaver, vil han ikke kunne delegere ansvaret.

I merknadene i Ot.prp. nr. 92 (1998-1999) s. 135 fremgår det at "[s]traffebudet omfatter både ansatte hos den behandlingsansvarlige og andre hjelpere som denne benytter (for eksempel databehandlere)". Dette kan tolkes som at slike

ansatte også er straffesubjekter i henhold til § 48. Etter FADs mening er dette en uriktig fordeling av straffeansvaret, og det vil være urimelig å tolke bestemmelsen i den retning. Riktig løsning må være at virksomheten pådrar seg ansvar også når det er ansatte eller hjelpere hos den behandlingsansvarlige som forsømmer sine plikter, men at det er den behandlingsansvarlige som er beheftet med straffeansvaret for dette.

Dette ville kommet tydeligere frem med følgende lovtekst:

"Med bøter eller fengsel inntil ett år eller begge deler straffes den *behandlingsansvarlige dersom han eller andre han svarer for,* forsettlig eller grovt uaktsomt..."

Elektroniske spor
At elektroniske spor legges igjen et uttall steder, byr på særskilte utfordringer. Enkeltindivider kan lett identifiseres og adferd kartlegges som følge av at vi på stadig flere områder legger igjen elektroniske spor. I denne forbindelse reises et spørsmål om det er nødvendig med en særskilt regulering av disse utfordringene, eller om andre lovendringsbehov utløses som følge av en stadig økende grad av elektroniske spor.

FAD mener at så lenge de elektroniske sporene kan knyttes til en enkeltperson, vil de også være å anse som personopplysninger, jf. pol. § 2 nr. 1.

Utrederne mener det er grunn til å oppmuntre behandlingsansvarlige til å velge teknologier som ikke innebærer behandling av elektroniske spor i form av personidentifiserbare opplysninger, og at de tar i bruk ordninger som raskt kan anonymisere eller pseudonymisere opplysningene (personvernfremmende teknologier). Behandlingsansvarlige bør oppfordres til ikke å behandle større mengder personopplysninger enn nødvendig, og å ta i bruk metoder som i størst mulig grad begrenser innsamling og behandling av personopplysninger, samt sørger for tilstrekkelig informasjonssikkerhet. FAD ser det imidlertid ikke som nødvendig å gjennomføre lovgivningsgrep som særskilt søker å begrense behandling av elektroniske spor. Lovgivning som hever terskelen for behandling av personopplysninger generelt sett, vil også få utslag for elektroniske spor. Vi viser her likevel til våre merknader i kap. **Feil! Fant ikke referansekilden.** om konsesjonsregulering av behandlinger i sektorer som behandler store mengder elektroniske spor.

Utrederne peker på at elektroniske spor ofte blir brukt til kontrollformål, og at dette kan være problematisk der dette ikke er primærformålet med innhentingen av opplysningene. Eksempelvis vil informasjon fra en teletilbyder om når og hvor telefonen har vært i bruk, kunne være interessant i markedsføringssammenheng. Utrederne nevner også arbeidsgiver som aktuell bruker av elektroniske spor til å

kontrollere arbeidstaker. FAD støtter utrederne i forslaget om at kontrollformål skal angis direkte for at den etterfølgende kontrollen skal være lovlig, slik dette framgår av det radikale lovforslaget § 9 annet ledd. Selv om dette ikke regulerer behandling av personopplysninger konkret, vil et slikt lovgivningsgrep fungere begrensende for bruk av opplysninger hentet fra elektroniske spor.

I utredningen trekkes det også frem at det er liten grad av selvbestemmelsesrett forbundet med elektroniske spor. Som deltaker i informasjonssamfunnet kan man ofte ikke velge å opptre anonymt. Elektroniske spor registreres i mange tilfeller uten at den enkelte er bevisst dette, og uten at det gis mulighet til å samtykke til eller nekte behandling av elektroniske spor. Opplysningene behandles ofte på bakgrunn av "nødvendig grunn" som rettslig grunnlag. FAD er enig i at "nødvendig grunn" ikke er et egnet rettslig grunnlag for behandling av elektroniske spor fordi dette er en type opplysninger som de registrerte ofte ikke har tilstrekkelig kunnskap om. Utrederne foreslår at dersom et reelt samtykke ikke er mulig å innhente pga. strukturell tvang, bør behandlingen skje på bakgrunn av lovhjemmel. FAD er enig i at dette kan gi et bedre rettsgrunnlag. Vi anbefaler ovenfor i kap. **Feil! Fant ikke referansekilden.** at de rettslige grunnlagene for å behandle personopplysninger strammes inn. Denne innstrammingen vil i så fall også begrense adgangen til å behandle elektroniske spor, slik at særregulering ikke er nødvendig.

Bruk av fødselsnummer, fingeravtrykk og annen biometri

Fødselsnummer

Bruk av fødselsnummer for autentisering (verifisering av identitet) har i mange år vært en kilde til diskusjon. Fødselsnummer er ikke en taushetsbelagt opplysning, og kan fremskaffes via mange lovlig tilgjengelige kilder. Det kan derfor synes problematisk å legge en rekke restriksjoner på bruk av fødselsnummer. Samtidig er det åpenbart at en offentlig tilgjengelig opplysning i utgangspunktet ikke egner seg til autentisering. Den senere tids utvikling med et økende antall identitetstyverier, som ofte synes å ha sin bakgrunn i misbruk av fødselsnummer, gir grunn til å mane til en viss varsomhet med tanke på bruk av opplysningen. All den tid fødselsnummer benyttes til autentisering til tross for at det er uegnet for slik bruk, er vi enig med utrederne i at det, gjennom lovregulering, er grunn til å forby slik bruk. Forbudet bør gjelde både i offentlig og privat sektor. Samtidig bør myndighetene benytte enhver anledning til å presisere at fødselsnummer ikke er en taushetsbelagt opplysning, og derfor er uegnet for autentiseringsformål. For identifikasjonsformål, vil fødselsnummer derimot være utmerket, siden opplysningen entydig identifiserer alle norske borgere, og skiller dem fra andre med samme eller svært like navn. I tjenester som ikke krever autentisering, men der identifisering er tilstrekkelig, bør det fremdeles være mulig å benytte fødselsnummer. Et eksempel på en slik tjeneste kan være bestilling av europeisk helsetrygdkort fra NAV. Om noen logger seg inn med en annens fødselsnummer og bestiller helsetrygdkort som sendes rette vedkommende, har dette neppe verken økonomiske eller rettslige konsekvenser. Hensikten med bruk av fødselsnummer i denne bestillingstjenesten, er kun å sørge for at kortet sendes til rette vedkommende. Bruk av fødselsnummer på denne måten bør fortsatt være tillatt.

Utrederne foreslår videre å endre bestemmelsen om at Datatilsynet kan pålegge bruk av fødselsnummer for å sikre opplysningskvalitet. Pålegg om bruk av fødselsnummer bør i følge utrederne i stedet være rettet mot å unngå personforveksling. Slik FAD ser det, er det å unngå personforveksling et element i kvalitetsaspektet. Fødselsnummer benyttes ofte i behandlinger av personopplysninger som innebærer kobling av flere registre. I denne sammenheng vil det å hindre personforveksling være nødvendig for å sikre opplysningskvalitet. Slik vi forstår forslaget, vil det være et bidrag til å snevre inn adgangen til å pålegge bruk av fødselsnummer. Dette skal bare kunne benyttes når det er nødvendig for å unngå personforvekslinger, og ikke når det ellers er nødvendig for å sikre opplysningskvalitet. FAD mener det ikke er nødvendig å legge denne begrensningen på Datatilsynets vurdering av i hvilke saker det kan være behov for bruk av fødselsnummer.

Personopplysningsforskriften § 10-2 inneholder i dag en bestemmelse om at postsendinger som inneholder fødselsnummer skal være utformet på en slik måte at nummeret ikke er tilgjengelig for andre enn adressaten. Bestemmelsen foreslås i forbindelse med lovrevisjonen flyttet opp i loven. Fokus på restriksjoner på bruk av fødselsnummer er ikke bare enkelt. Etter FADs vurdering er det ikke ønskelig å overdramatisere farene ved bruk av fødselsnummer forutsatt at opplysningen brukes riktig. Samtidig er det på det rene at det er knyttet visse ulemper til ufornuftig bruk av fødselsnummer. Som nevnt i avsnittene om personopplysningslovens struktur, finner vi det imidlertid ikke hensiktsmessig å flytte bestemmelser fra forskriften og opp i loven. Som tiltak for å forhindre misbruk av fødselsnummer, mener vi derimot staten må arbeide aktivt for en holdningsendring knyttet til bruk av fødselsnummer. All den tid fødselsnummer ikke er en taushetsbelagt opplysning, er det av stor betydning at nummeret ikke aksepteres som en nøkkel til annen taushetsbelagt informasjon om vedkommende. Dette er en naturlig konsekvens av at nummeret er helt uegnet for autentiseringsformål. Særlig viktig er dette i tider da vi ser en økning i antall id-tyverier. FAD mener derfor at det som hovedregel bør utformes en positiv bestemmelse som sier at fødselsnummer kan brukes for identifisering, men ikke er tilstrekkelig for å autentisere en bruker.

Bestemmelsen om at fødselsnummer ikke må stå utenpå brevsending, som foreslås flyttet fra forskriften til loven (se våre merknader om dette ovenfor), er i utredernes forslag (utkastets § 11, 5. ledd) endret til at "enhver forsendelse som inneholder fødselsnummer skal være utformet slik at nummeret ikke er tilgjengelig for andre enn adressaten". Dette er både et overraskende og vidtrekkende forslag og vil innebære at fødselsnummer som sendes via e-post må krypteres, noe som vel ikke kan ha vært utredernes mening.

Avslutningsvis vil FAD gi uttrykk for noen generelle betraktninger knyttet til bruk av fødselsnummer. Fødselsnummer er ikke en taushetsbelagt opplysning. Dette kommer blant annet til uttrykk i forvaltningsloven, der fødselsnummer ikke er blant de

opplysningene som er underlagt taushetsplikt. Likevel eksisterer det en oppfatning i samfunnet om at nummeret er en taushetsbelagt opplysning, og det tillegges legitimasjonsvirkning. Utredernes lovforslag kan også sees på som uttrykk for en oppfatning om at fødselsnummer bør behandles som en sensitiv og "hemmelig" opplysning. En opplysning som av svært mange oppfattes som "hemmelig" og taushetsbelagt, og som det til stadighet gis uttrykk for at man bør behandle med varsomhet og ikke gi til uvedkommende, bør kanskje nettopp være en taushetsbelagt opplysning. Dersom man ønsker dette, må det i så fall konsekvensutredes. FAD ber på denne bakgrunn om at JD, som lovansvarlig for forvaltningsloven, vurderer om fødselsnummerets status som en ikke taushetsbelagt opplysning, bør endres før det innføres flere regler som underbygger oppfatningen om fødselsnummerets hemmelige status.

Biometri

I rapport II foreslås ny bestemmelse om bruk av biometri, § 12. Det foreslås strenge begrensninger på adgangen til å benytte biometri både til identifisering og autentisering. Personopplysningsloven § 12 er i følge Datatilsynet utformet med henblikk på å hindre misbruk av fødselsnummer, men i forarbeidene nevnes biometri som eksempel på et entydig identifikasjonsmiddel. Datatilsynet er imidlertid av den oppfatning at forarbeidene ikke tok høyde for de egenskapene biometri har i forhold til også å autentisere brukere. Datatilsynet har derfor ytret ønske om endring av loven slik at man får en avklaring på hvordan man skal forholde seg til den økende pågangen rundt biometriske system. Samtidig har forvaltningspraksis fra Personvernnemnda også vist en relativ positiv holdning til biometri.

Fordelene med biometriske mønstre er at de er uløselig knyttet til en persons fysiske karakteristika og dermed godt egnet til sikker identifisering og autentisering: man kan ikke miste eller glemme slike. Det er også atskillig vanskeligere eventuelt å få frastjålet slike karakteristika. Dermed reduserer man sjansene for identitetsmisbruk. På den andre siden vil konsekvensene sannsynligvis blir ekstra belastende nettopp fordi biometriske kjennetegn som metode er ansett for å være svært sikker og dermed i) vil kunne gi tilgang til mye informasjon og ii) gjøre det vanskelig å bli trodd dersom man hevder man er blitt utsatt for misbruk. Identitetstyveri hvor biometriske mønstre er inkludert, vil dermed være en større utfordring å håndtere enn tradisjonelle autentiseringsfaktorer som brukernavn og passord.

Utfordringene med bruk av biometri kan knyttes til dårlig teknologi eller menneskelig svikt, og særlig utsatte områder er både innrullering av brukere og senere autentisering. Korrekt setting av parametre for gjenkjenning av individer er avgjørende for hvordan et biometrisk system fungerer. Videre er måten biometriske templater produseres, lagres og brukes på et område som kan ha stor innvirkning for sikkerheten mot misbruk. Mange betrakter biometri som en rask, effektiv og sikker løsning for å bekrefte at en person er den hun eller han utgir seg ut for å være. Det er også viktig å

påpeke at biometriske løsninger i mange sammenhenger oppfattes av brukere som enkle og lettvinte å bruke.

Samtidig kan bruk av biometri være et godt bidrag til å utvikle sikre løsninger mot autentisering av feil person og dermed motvirke eksempelvis identitetstyveri. Forutsetningen for at biometri er et godt tiltak er imidlertid at løsningene som benyttes er sikret mot misbruk i forhold til risikoen for det. Risiko for misbruk vil være uløselig knyttet til konteksten biometrien skal brukes i. Det blir derfor svært viktig å vurdere på hvilke områder og i hvilke sammenhenger det er hensiktsmessig og rimelig trygt å benytte denne teknologien, og hvor det ikke er tilrådelig.

I kombinasjon med noe personen har eller vet, vil biometri kunne gi svært god sikkerhet ved autentisering (og dermed motvirke ID-tyveri). Man kan imidlertid også se for seg løsninger som benytter biometri for å autentisere en tilbakevendende bruker uten at denne blir identifisert og uten at sporene etter autentiseringen skal lagres eller kobles opp mot andre opplysninger på annet vis enn i selve autentiseringsøyeblikket. Teknologien kan brukes anonymt, for eksempel som "nøkkel" i et garderobeskap eller ved adgangskontroll uten at dette nødvendiggjør registrering av personopplysninger.

Mye av teknologien begynner å bli moden for å tas i bruk. Samfunnet trenger erfaringer med denne teknologien for at gode og hensiktsmessige reguleringstiltak skal kunne vurderes og implementeres. En streng a priori regulering av bruken av biometri vil redusere denne muligheten.

Bruk av biometri synliggjør spenningsforholdet mellom utvikling av ny teknologi og et godt personvern. Mange vil oppleve bruk av biometri som svært inngripende. Personvernhensyn kan derfor tilsi at det bør foreligge lovhjemmel eller samtykke ved bruk av løsninger basert på biometri. Det kan også anføres at inngrep av denne typen i borgernes integritet må ha hjemmel i lov, ev. være basert på samtykke, for ikke å komme i konflikt med legalitetsprinsippet. På denne bakgrunn mener FAD at den foreslåtte reguleringen kan få utilsiktede konsekvenser, og at området derfor må utredes ytterligere før det kan lovreguleres.

Utrederne foreslår en særskilt regel om sletting av biometriske data for avdøde personer, forslaget § 28a. FAD antar at det sjelden vil foreligge saklig behov for videre lagring av biometriske data for avdøde, annet enn i situasjoner der det finnes særskilte regler (typisk pass, asylsaker og lignende). Opplysningene skal derfor, i samsvar med de generelle reglene om behandlingsgrunnlag, slettes når den registrerte dør. FAD ser imidlertid at slik sletting dessverre ikke alltid blir gjort, og sletteplikten for personopplysninger om avdøde personer kan derfor med fordel presiseres i regelverket. Det er FADs vurdering at de generelle slettereglene også vil regulere plikten til å slette biometri.

Utrederne foreslår videre en særskilt regel om objektivt erstatningsansvar for skader som oppstår som følge av mangelfull sikring av fødselsnummer og biometriske data. Regelen vil være tilsvarende som for uriktig utlevering av kredittopplysninger. Bestemmelsen vil plassere ansvaret for mangelfull sikring på den behandlingsansvarlige uavhengig av utvist skyld. Dette vil trolig kunne virke oppdragende. Økonomisk ansvar i tillegg til negativ publisitet ved ev. sikkerhetsbrudd vil forhåpentligvis føre til at behandlingsansvarlige sikrer løsningene sine så godt det lar seg gjøre. FAD støtter derfor den foreslåtte bestemmelsen om erstatningsansvar for skader oppstått som følge av mangelfull sikring av fødselsnummer og biometriske data.

11. ØKONOMISKE OG ADMINISTRATIVE KONSEKVENSER

Ut fra de lovendringsforslagene vi anbefaler, ser vi at Datatilsynet kan få noen økte kostnader. Dette kan f.eks. gjelde kostnader i forbindelse med endret meldesystem. Dersom de endelige lovendringene viser økte kostnader for tilsynet, må FAD ta forbehold om at det finnes dekning for disse i de alminnelige budsjettprosessene før forslagene gjennomføres.

Med hilsen

for Bjørn Magnus Jakobsen (e.f.)
fung. avdelingsdirektør

Anne Kristine Hage
rådgiver