1/83

ARVE FØYEN

UTREDNING OM ENDRINGER I PERSONREGISTERLOVEN

COMPLEX

JUSTISDEPARTEMENTET

UNIVERSITETSFORLAGET

Jon Bing

CompLex nr. 1/83

Justisdepartementet

Arve Føyen

UTREDNING OM ENDRINGER I PERSONREGISTERLOVEN

Universitetsforlaget
Oslo

ISBN 82-00-06552-9

Printed in Norway by LOBO, Oslo

FORORD

Personregisterloven har nå vært i kraft i tre år. Det har blitt stadig mer klart at det er et misforhold mellom de ambisjoner personregisterloven legger opp til for å kontrollere at personverninteresser blir ivaretatt, og de ressurser (særlig personellmessige) som har blitt stilt til rådighet for å gjennomføre denne kontrollen.

Videre er det åpenbart at det i årene etter at personregisterloven ble vedtatt, har forgått en rivende teknisk utvikling. Denne utviklingen har ført til at deler av personregisterloven passer relativt dårlig for å ivareta personverninteresene, samtidig som den har ført til drastiske økninger i arbeidsoppgavene for Datatilsynet.

Justisdepartementet ba derfor ved brev av 6.4.82, undertegnede om å utføre en utredning av mulighetene for forenklinger, av økte problemer ved den betydelige økningen i utbredelse av dataanlegg, og av Datatilsynets erfaringer med loven hittil, med sikte på avklaring av tvilsspørsmål. Fullstendig mandat er gjengitt i avsnitt 1.1 i utredningen.

Utredningen er gjennomført i tiden fra 1.5.82 til 31.12.82.

Til å bistå meg med råd og veiledning, opprettet departementet en referansegruppe bestående av direktør Kåre Fløisand, professor Knut S. Selmer, underdirektør Eva Nygaard Ottesen og byråsjef Jon Bonnevie Høyer. Referansegruppen har hatt 5 møter der utkast til de forskjellige delene av utredningen har vært fremlagt og diskutert. Gruppens synspunkter har vært til stor hjelp i arbeidet med utredningen.

Under gjennomføringen av utredningen har jeg disponert kontorlokaler og tekstbehandlingsutstyr i Datatilsynet. Derved har jeg også fått verdifulle impulser til mitt arbeid.

Den endelige utformingen av utredningen er imidlertid fullt ut mitt eget ansvar, på samme måte som jeg alene innestår for de løsninger som foreslås i utredningen.

Endelig vil jeg understreke at det har vært nyttig og interessant for meg personlig å få anledning til å foreta en såvidt omfattende gjennomgang av problemstillingene, idet jeg forlater Datatilsynet for å begynne som advokatfullmektig i januar 1983.

Oslo, desember 82

Arve Føyen

Innhold

DATATILSYNET NOTAT

AF 9.12.82

1. INNLEDNING - OVERSIKT

1.1. Utredningsoppdrag

Ved brev av 6.4.82 fra Justisdepartementet, er utredningsoppdraget angitt på følgende måte:

a) Utrede mulige endringer i regelverk (lov og forskrifter) og administrative rutiner som kan foretas for å begrense Datatilsynets arbeidsbyrde uten at det i vesentlig grad antas å ville ha uheldige virkninger for personvernet.

b) Utrede hvilke problemer den betydelige utbredelse av dataanlegg, spesielt mikromaskiner, kan ventes å medføre i de nærmeste år. Det gjelder både problemer knyttet til personvernet, og problemer knyttet til administrasjonen av regelverket, såvel for Datatilsynet som for brukerne av dataanlegg.

c) Gjennomgå Datatilsynets erfaringer hittil, med sikte på å kartlegge tvilsspørsmål som har oppstått, og som det er viktig å få avklart for Datatilsynets virksomhet. Forslag til løsninger ønskes utarbeidet der det er mulig innen prosjektets ressursrammer.

Jeg ser det slik at pkt. a) tar sikte på forenklinger av virksomheten i dagens situasjon og med sikte på den nære fremtid, pkt. b) tar sikte på å lage en beredskap for den utviklingen vi er inne i, mens pkt. c) tar sikte på å få en belysning av konkrete tvilsspørsmål som personregisterloven i sin nåværende utforming har medført.

1.2. Sammendrag - oversikt over fremstillingen

Utredningen gjelder forenkling og tilpasning av personregisterloven, for å bringe bedre overensstemmelse

mellom Datatilsynets arbeidsoppgaver og tilgjengelige ressurser, sett på bakgrunn av den teknologiske utvikling vi står overfor. Innledningsvis redegjøres det i avsnitt 1.3 for hva "personvern" er. Personvern er en mulig interesse fra enkeltpersoners side i å utøve kontroll med den informasjon som beskriver dem. Denne kan spaltes videre opp i interessen i:

- diskresjon
- fullstendighet
- å være opplyst
- å ha en "borgervennlig administrasjon"
- å unngå overdreven kontroll.

I avsnitt 1.3.2 knyttes det en del kommentarer til motsetningene mellom en utvikling i retning av et åpent samfunn med enkle relasjoner mellom den enkelte og samfunnet på den ene side, og en utvikling i retning av et kontrollsamfunn med stadig mer komplekse relasjoner mellom samfunnet og den enkelte på den annen side. Det påpekes at personvern inneholder fler av de samme elementer som de tradisjonelle rettssikkerhetsgarantiene. Videre påpekes det at en utvikling i retning av et kontrollsamfunn, med utstrakt overføring av opplysninger mellom offentlig og privat sektor, og mellom forskjellige enheter innenfor hver av disse sektorene, vil medføre betydelige problemer ut fra rettssikkerhetshensyn. Videre påpekes det at man med en etter hvert omfattende registrering av informasjon om hva personer til en hver tid foretar seg, kan komme opp i en situasjon hvor registeropplysningene sannsynliggjør bestemte handlinger (f.eks. noe som ser ut som straffbare handlinger), med den følge at den enkelte må bevise sin uskyld (vi får en "omvendt bevisbyrde" for straffbare handlinger).

Kapittel 2 i utredningen inneholder en redegjørelse for noen viktige problemer som oppstår pga. den stadige aksellererende utviklingen av EDB-teknologien, og i forbindelse med noen viktige bruksområder for denne teknologien. Følgende emner diskuteres ut fra interessene til registereierne, Datatilsynet som kontrollinstans og personvern- interessene:

- elektronisk tekstbehandlingsutstyr
- mikromaskiner
- systemer for registrering av tjenestebruk
- elektronisk post og teledocsystemer
- betalingsformidling
- salgspunktterminaler
- on-line diagnose og feilretting av EDB-utrustning
- teledata - tekst-tv
- systemer for søking i fri tekst

Det understrekes at det bare er et begrenset utvalg av problemer som er tatt opp i utredningen. Videre understrekes det at det er særdeles viktig for Datatilsynet å følge med i den utvikling som skjer på slike nye områder, for ikke å bli hengende etter den tekniske utviklingen og bli et "sandpåstrøingsorgan" for løsninger fastlagt av andre. Det understrekes videre at

Datatilsynet ut fra sine arbeidsoppgaver i dag ikke har ressurser til å kunne utføre systematisk arbeid med sikte på å holde seg ajour med den tekniske utviklingen.

En viktig begrensning ved denne utredningen, er at den i følge sitt mandat, og pga. den tid som har stått til rådighet for utredningen, kun har tatt for seg den tekniske utviklingen på et begrenset felt. Således behandler utredningen ikke de store offentlige og private registeroppleggene som i sin tid var bakgrunnen for at vi fikk en personregisterlov. Det understrekes at den tekniske utviklingen har betydd mye også for de tradisjonelle "personregistrene". Pga. pris/ ytelsesutviklingen og sterkt forbedrede programmer, er det i dag betydelig rimeligere å lagre store datamengder, og å sammenstille opplysninger fra forskjellige kilder. Behovet for kontroll med innsamling lagring og bruk av personopplysninger, er derfor i dag minst like stort, om ikke vesentlig større som det var da personregisterloven ble forberedt i midten av 1970-årene. Dette er en utvikling som vil fortsette i årene som kommer.

I kapittel 3 redegjøres det for mulige endringer som kan foretas i regelverket. I avsnitt 3.1 påpekes det at det er lite å vinne ved å foreta ytterligere effektivisering av arbeidet i Datatilsynet. Effektiviseringen er her ført så langt som det er forsvarlig ut fra någjeldende regelverk. Videre påpekes det at regelverket i forbindelse med personregisterloven er såvidt komplisert i sin utforming, at det er vanskelig for publikum å orientere seg i det. Ytterligere forsøk på å begrense Datatilsynets arbeidsbyrde ved å gi forskrifter, avskrives derfor, fordi det vil føre til en økende kompleksitet. Den videre fremstillingen i kapittel 3 konsentreres derfor om grunnleggende endringer i selve personregisterloven. Det påpekes at bare gjennom slike endringer vil Datatilsynets arbeid kunne forenkles vesentlig.

I avsnitt 3.2 redegjøres det for hvordan personvern-interessene er ivaretatt gjennom bestemmelsene i den någjeldende personregisterloven.

I avsnitt 3.3 påpekes det at det må stilles visse krav til presisjonsnivået for materielle regler som skal sanksjoneres med straffebestemmelser. Dette er en viktig begrensning ved adgangen til å erstatte den nåværende konsesjonsordningen med vage, skjønnsmessige materielle regler, som er sanksjonert med straff.

I avsnitt 3.4 redegjøres det nærmere for personregister-lovens opplegg for kontroll med personregistre. Loven bygger i dag på at vi har enkelte, til dels skjønnsmessige, materielle bestemmelser i loven, samt et vidtgående konsesjonssystem med vide fullmakter for Datatilsynet til etter fritt skjønn å vurdere hva som er relevante opplysninger, til å gi regler om bruk, oppbevaring, behandling, sletting, sikring osv. av opplysningene. Det redegjøres nærmere for sammenhengen mellom dette systemet, og de kravene som følger av

legalitetsprinsippet.

Det konkluderes med at et system basert på forholdsnormer - som skal gjelde generelt for alle typer personregistre - fremdeles må være såvidt generelt utformet at det vil være vanskelig å understøtte det med straffesanksjoner.

I avsnitt 3.5 redegjøres det for synspunkter som har fremkommet i Stortinget om endring av enkelte bestemmelser i personregisterlovgivningen. Videre redegjøres det nærmere for de krav som stilles til lovgivningen på dette området pga. internasjonalt samarbeid.

I avsnitt 3.6 redegjøres det nærmere for prinsipielt forskjellige alternativer som kan legges til grunn ved regulering av personvernspørsmålene. Innledningsvis drøftes spørsmålet om Datatilsynets avhengighet/selvstendighet i forhold til resten av forvaltnings-apparatet. Dernest diskuteres følgende alternative opplegg for kontroll med innsamling, lagring og bruk av personopplysninger:

- Materielle bestemmelser om innsamling, lagring og bruk av personopplysninger - uten noe eget organ til å følge opp bestemmelsene.

- Materielle bestemmelser kombinert med opprettelse av en ombudsmann underlagt Stortinget.

- Materielle bestemmelser - opprettelse av en ombudsmann som kan avgi uttalelser om personvernspørsmål.

- Materielle bestemmelser - kombinert med et organ som har beslutningsmyndighet i forhold til de som ønsker å foreta innsamling, lagring og bruk av personopplysninger.

Under den sistnevnte varianten diskuteres henholdsvis et opplegg uten noen nærmere meldeplikt eller konsesjonsplikt, et opplegg med fastlagte rammer for hva som er tillatt, kombinert med en dispensasjonsadgang, et opplegg med meldeplikt for de som skal opprette samlinger av person- opplysninger, og et opplegg med en konsesjonsordning.

I avsnitt 3.7 gis det anbefalinger om valg av alternativ. Innledningsvis konkluderes det med at det beste alternativ (ut ifra ivaretakelse av personverninteressene) for regulering av bruk av personopplysninger fortsatt er det system som vi har i personregisterloven i dag: enkelte, relativt vage forholdsnormer - kombinert med konsesjonsplikt eller evt. forskriftsregulering av individuelle registre/registertyper. Dernest redegjøres det for behov for personalressurser for gjennomføring i dagens situasjon av de ulike alternativene som det er redegjort for. Det påpekes at en fornuftig gjennomføring av dagens opplegg, ville kreve at Datatilsynet totalt må ha ca. 20 ansatte personer. Dette vil medføre direkte kostnader til

Datatilsynet på et sted mellom 6 og 7 mill. kr. pr. år (totalt).

Det påpekes at en av grunnene til gjennomføringen av utredningsprosjektet, er at det i overskuelig fremtid ikke er aktuel å øke staben i Datatilsynet noe særlig ut over dagens antall (8 personer). Med denne ressursmessige forutsetningen, konkluderes det i avsnitt 3.7.3 med at personvern- interessene best mulig kan ivaretas ved at personregisterloven bygges ut med enkelte mer presise materielle regler enn dagens lov, at Datatilsynet opprettholdes som et organ med ombudsmannsfunksjoner og med myndighet til å gripe inn ved forbud mot ulovlig innsamling, lagring og bruk av opplysninger, og som har vide fullmakter til å kreve opplysninger og til å gjøre kontroller hos de som samler inn, lagrer eller bruker opplysninger. Videre bør det ha myndighet til å nedlegge forbud, og til å oppstille vilkår for å få lov til å fortsette med bestemt virksomhet.

I avsnitt 3.8 gis det en nærmere vurdering av den foreslåtte endringen sett i forhold til den nåværende ordningen, ut fra de foreliggende ressursforutsetninger for Datatilsynet.

Kapittel 4 inneholder en gjennomgang av tvilsspørsmål som har reist seg i forbindelse med tolkning av personregisterloven, samtidig som kapitlet inneholder et forslag til konkrete endringer i lovteksten i personregisterloven ut fra den endringen som er foreslått i avsnitt 3.7, og ut fra den teknologiske utviklingen. På grunnlag av diskusjonen om Datatilsynets avhengighet av forvaltningen, foreslås det at myndighet til å gi forskrifter og treffe enkeltvedtak etter loven legges direkte til Datatilsynet, og til styret i Datatilsynet (uavhengig av departementet).

I kapittel 1 foreslås registerbegrepet opphevet, og loven skal i stedet gjelde all innsamling, lagring og bruk av personopplysninger, og visse typer virksomhet. Videre innføres det en hjemmel til å gi forskrifter om innsamling, oppbevaring og bruk av personopplysninger som foretas av privatpersoner.

I kapittel 2 foreslås det to prinsipielt forskjellige måter å organisere Datatilsynet og styret for Datatilsynet på. Valg av alternativ vil her avhenge av om Datatilsynet skal ha en helt selvstendig kompetanse uavhengig av forvaltningen, eller om det skal være underlagt alminnelig instruksjonsmyndighet fra regjeringen (eller departementet). § 4 om opprettelse av en egen fortegnelse for personregistre, foreslås opphevet. I tilknytning til § 5 som inneholder bestemmelser om Datatilsynets kontrolladgang, påpekes at det hefter spesielle problemer med unntak for registre som føres av hensyn til rikets sikkerhet mv., og at det bør etableres et samarbeid mellom Datatilsynet og kontrollutvalget for overvåknings- og sikkerhetstjenesten.

I kapittel 3 foreslås det en rekke regler av materiell karakter. Således innføres det bestemmelser om at opplysninger som samles inn, lagres eller brukes for et formål, ikke må utnyttes for andre formål uten utrykkelig samtykke eller særlig lovhjemmel, at opplysninger ikke må leveres ut annet enn i spesielt oppregnede tilfelle, at personopplysninger ikke må kobles sammen med andre opplysninger annet enn i spesielt oppregnede tilfelle, om at en person kan kreve sitt navn sperret mot bruk til utsendelse av direkte reklame og andre publikasjoner, om at øverste administrative leder av den virksomhet der personopplysninger samles inn, lagres eller brukes, er ansvarlig for at reglene i personregisterloven overholdes og er ansvarlig for tilstrekkelig sikring av opplysninger, at det kan gis forskrifter om sikringstiltak for innsamling, lagring og bruk av personopplysninger i helt generell form, visse endringer i reglene om innsynsrett for den enkelte, samt en regel om at Datatilsynet ved forskrift eller enkeltvedtak kan gjøre unntak fra de materielle bestemmelsene, og fastlegge nærmere vilkår for innsamling, lagring og bruk av opplysninger som omfattes av et slikt unntak. Videre foreslås det at Datatilsynet ved forskrift eller ved enkeltvedtak kan nedlegge forbud mot innsamling, lagring eller bruk av personopplysninger og fastlegge nærmere vilkår i tilknytning til en slik innsamling, lagring eller bruk.

Kapittel 4 i loven (om konsesjonsplikt) foreslås opphevet i sin helhet. Det påpekes at det er vanskelig å vurdere om den foreslåtte endringen vil gi tilstrekkelig ivaretakelse av personverninteressene, men at en ordning som den foreslåtte sannsynligvis vil gi bedre personvern enn dagens ordning, dersom Datatilsynets ressurser skal være uendret.

Det foreslås bare mindre endringer i de øvrige bestemmelsene i loven.

Før jeg går nærmere inn på de enkelte punkter i utredningen, vil jeg redegjøre nærmere for begrepet "personvern", slik det etterhvert er blitt vanlig å forstå det i vår sammenheng.

1.3. Personvern

1.3.1. Hva er personvern

Min fremstilling i det følgende bygger først og fremst på to artikler av hhv. Ragnar Dag Blekeli og Knut Selmer, inntatt i boken "Data og personvern" (Universitetsforlaget 1977), s. 13 flg. og s. 27 flg. Som fremhevet av Blekeli, kan personvern i utgangspunktet sees som en mulig interesse fra enkeltpersoners side i å utøve kontroll med den informasjon som beskriver dem.

Etter Blekelis oppfatning er det først når personopplysninger faktisk blir brukt, eller kan forventes å bli brukt, at sirkulasjonen av personinformasjon får konsekvenser for den enkelte.

Blekeli benytter i denne sammenheng begrepet "beslutning" i meget vid forstand, slik at det omfatter såvel formelle beslutninger truffet av forvaltningsorganer, private bedrifter mv., som sosiale reaksjoner fra arbeidskamerater e.l.

Blekeli påpeker at konsekvensen av avgjørelser kan berøre den enkelte i ulik grad: Jo mer resultatet av en avgjørelse griper inn i ens livssituasjon, jo mer interessert vil en være i den - og desto mer vil det bety for en at avgjørelsen treffes på et korrekt grunnlag, og på måter som en kan akseptere. Dette fører etter Blekelis oppfatning til at personvern blir en del av spørsmålet om "fair saksbehandling."

I sin videre analyse av personvernbegrepet, spalter Blekeli det opp i tre "interesser", som individet har.

For det første vil det være visse opplysninger som vedkommende mener ikke har noe med den aktuelle saken å gjøre. Isåfall vil han/hun være interessert i å sette restriksjoner på bruken av disse opplysningene i saken. Vedkommende vil med andre ord være interessert i diskresjon, eller i å begrense de aktuelle beslutningstakernes tilgang til personopplysninger.

For det andre vil den enkelte være interessert i at alle de opplysninger som har betydning for saken, blir tatt i betraktning. Med andre ord: beslutningsgrunnlaget må være så fullstendig som mulig. Fullstendighet impliserer selvfølgelig også at opplysningene må være korrekte, aktuelle og tilstrekkelig presise.

For at den enkelte skal ha en mulighet til å ivareta sine to forannevnte interesser, (diskresjon, og fullstendighet), må vedkommende vite om at det treffes (vil bli truffet) bestemte typer beslutninger som vedrører ham/henne. Videre er det nødvendig å vite hva som er formålet med beslutningene, og hvilke opplysninger om en selv som legges til grunn for den avgjørelsen som treffes. Dette leder fram til den tredje av de interesser personvernet kan sies på bestå av: interessen i å være opplyst.

Blekelis synspunkter bygges videre ut av Selmer. I tillegg til de tre ovennevnte interessene, påpeker Selmer at den enkelte - selv om han/hun ikke kan påvirke administrasjonen (beslutningsfatteren) - må kunne forlange å bli møtt med et vennlig ansikt. Han påpeker at den enkelte har en klar interesse i at avgjørelser blir truffet raskt, at de blir skikkelig motivert, at motforestillinger kan fremføres på hjemstedet og for en velutdannet og velinformert person, som taler et forståelig språk. Videre påpekes interessen i at administrasjonen er rettferdig, i den forstand at det

treffes riktige avgjørelser i henhold til det regelverk som skal anvendes. Selmer sammenfatter dette i det han kaller interessen i en borgervennlig administrasjon.

Ytterligere en interesse betones relativt sterkt av Selmer: interessen i å unngå overdreven kontroll og uhjemlet maktbruk. På sett og vis kan vel denne interessen til en viss grad sies å inneholde alle de forannevnte, slik at den mer blir en spesiell sammensetning av de øvrige interessene. Etter min oppfatning er den imidlertid velegnet som bakgrunn for vurdering av enkelte utviklingstendenser som trer stadig mer i forgrunnen i vårt høyt utviklede og stadig mer komplekse samfunn. På et raskt økende antall områder - enten det gjelder tilståelse av goder eller påleggingav byrder - vil administrasjonen (offentlig forvaltning såvel som private bedrifter mv.) sakte men sikkert få økt sine muligheter til å kontrollere at opplysninger den enkelte gir i søknadsskjemaer, egenmeldinger mv., stemmer med det vedkommende har meldt fra om i andre sammenheng, ved at det foretas kobling av registre.

Sett ut fra ønsket om å bekjempe den del av den økonomiske kriminalitet som retter seg mot det offentliges midler, er det selvsagt ønskelig å ta de foreliggende hjelpemidler i bruk.

Det er imidlertid etter min oppfatning grunn til å understreke at en stor del av denne kriminaliteten blir muliggjort på grunn av samfunnets økende kompleksitet. Den kan derfor ikke sees på som avgrensede kontroll- og sanksjonsspørsmål. Et sentralt spørsmål blir derfor om det er mulig - eller endog ønskelig - å kontrollere og straffe bort disse formene for økonomisk kriminalitet. Det grunnleggende problemet kan antakelig bare løses gjennom fundamentale endringer i det regelverk som ligger til grunn for samfunnets virksomhet på de aktuelle områdene - endringer som tar sikte på vesentlige forenklinger av reglene, samtidig som det i vesentlig grad tas hensyn til at reglene skal være enkle å iverksette og kontrollere. Istedet for ensidig å sette inn ressurser på kontroll, bør etter dette større ressurser settes inn for å forenkle samkvemmet mellom den enkelte og myndighetene.

Flere av de interessene som den enkelte har etter det som er sagt ovenfor, vil ofte være sammenfallende med interessene til den som fører det aktuelle register: Organer for stat og kommune er einteressert i fullstendige og korrekte opplysninger for å kunne treffe riktige og velbegrunnede avgjørelser. Sosialetatene er interessert i forsvare sine taushetsregler, for å kunne nyte den nødvendige tillit hos sitt klientell, slik at de kan utføre sine oppgaver best mulig. De som fører registre er interessert i å slette overflødig informasjon, for å begrense ressursforbruket osv.

1.3.2. Åpent samfunn - kontrollsamfunn

Jeg vil knytte noen få kommentarer - delvis basert på materiale som er stilt til rådighet i samtaler jeg har hatt med representanter for den svenske Datainspektionen - til den konflikten som ser ut til å tilspisse seg mellom forkjempere for et åpent samfunn med enkle relasjoner mellom den enkelte og samfunnet på den ene side, og forkjemperne for kontrollsamfunnet, med stadig mer komplekse relasjoner mellom samfunnet og den enkelte på den annen side.

Den økonomiske veksten i samfunnet har avtatt i de senere år. Kostnadene for velferdssamfunnets goder stiger. Bl.a. krever et komplisert regelverk, og en økende innbyrdes avhengighet mellom forskjellige sett av ordninger, at det satses betydelige midler på utbygging av omfattende administrative ordninger som krever store ressurser. En av de sterkeste innvendingene mot innføring av den så mye omtalte båtavgiften, har vært at samfunnets netto gevinst ved ordningen, har vært forsvinnende liten.

Fra mange hold gjøres det med stadig økende styrke gjeldende at enkeltpersoner snylter på velferdssamfunnets goder. Jeg tviler i og for seg ikke på at dette er sant nok. På den annen side er det dokumentert gjennom flere undersøkelser at mange (sannsynligvis fler enn snylterne) mangler forutsetninger til å kunne ivareta sine rettigheter overfor samfunnet, og ennå mindre til å sette seg inn i sine plikter overfor det. Gjeldende regelverk er på mange områder blitt så komplisert - og forandringstakten så sterkt økende - at selv trenede jurister har store vansker med å holde seg orientert på enkelte sentrale områder. Ikke desto mindre fremmes det stadig mer høylydte krav om at snylterne skal gripes og stå til rette for sine ugjerninger.

Med det utrolig slagkraftige nye hjelpemidlet EDB, er det etterhvert blitt mulig å tillempe svært kompliserte stønads- og avgiftsregler - og å samordne dem innbyrdes i konkrete saker. For å hindre snylting, ligger det imidlertid nær å sette iverk forskjellige kontrolltiltak.

Kobling (samkjøring) av forskjellige myndigheters personregistre er et meget effektivt kontrolltiltak. Slik kobling kan gjennomføres uten store kostnader (sett i forhold til omfanget av kontrollen). Kobling av personregistre foretas imidlertid på en slik måte at også aktsomme og lojale samfunnsborgere blir kontrollert - og de blir kontrollert uten at de selv vet om det. Tidligere har det vel nærmest vært en hovedregel at myndighetene kontrollerte når det forelå skjellig grunn til mistanke om ulovligheter. Det ser ut til å bli stadig vanskeligere å argumentere mot slike koblinger for kontrollformål ut ifra de mer diffuse "personverninteressene", slik disse er gjengitt ovenfor.

Det man dessuten bør vie atskillig større oppmerksomhet framover enn man har gjort til idag, er ulikhet i de begreper som anvendes i de forskjellige EDB- registre.

"Inntekt" kan være så mange forskjellige ting. Brutto inntekt, brutto skattbar inntekt, netto inntekt, netto skattbar inntekt, pensjonsgivende inntekt, brutto inntekt som grunnlag for beregning av barnehageavgift (inkluderer i enkelte kommuner bl. a. lån i Statens lånekasse) osv. Et annet godt eksempel er begrepet "rimelige boutgifter" i bostøtteordningens forstand, som er noe helt annet enn det man vanligvis ville legge i begrepet "rimelige boutgifter." Slike forskjeller i begrepsbruken kan jurister oppdage og vurdere. Man kan imidlertid etter min oppfatning ikke kreve at alminnelige mennesker, idet de sitter og sliter over et eller annet skjema fra en eller annen myndighet som ber om oppgave over inntekt eller over boutgifter, til enhver tid skal kunne holde seg etterrettelig hvilket begreo som legges til grunn.

Jeg vil dessuten våge den påstand at heller ikke de som utformer kontrolltiltak (les: foreslår kobling av personregistre for kontrollformål), er særlig flinke til å forsikre seg om at det er samsvar i begrepsbruken, når de f.eks. foreslår at "inntekt" registrert i to forskjellige registre opprettet for to forskjellige formål, skal kontrolleres mot hverandre.

Dessverre forekommer det ofte at EDB-registrene inneholder gale opplysninger, eller opplysninger som ikke passer for det kontrollformål som de ønskes benyttet til. Hederlige samfunnsborgere som på denne måten "hektes", tvinges da til å bevise overfor myndighetene at de ikke har gjort noe galt. Det er riktignok at "personvernet" ikke skal benyttes for å skjule bedragersk virksomhet, men det må ropes et alvorlig varsko når bevisbyrden for kriminelle handlinger snus opp ned i forhold til hva vi har vært vant til. Dette må særlig gjøres gjeldende ettersom den enkelte i alle henseende har en meget svak stilling i forholdet til det offentlige, med sine eksperter og spesialister.

Riktignok kan det hevdes at den enkelte vil få sin sak opp for domstolene på vanlig måte, og at alle de vanlige rettssikkerhetsmekanismene vil settes i sving. Dette er imidlertid en mager trøst for et alminnelig menneske, som før det kommer så langt har hatt betydelig bryderi og mange ulemper. Hva skal dessuten den enkelte stille opp med av beviser for å sannsynliggjøre at myndighetene (les: EDB - systemene) tar feil?

Det kan hevdes at en restriktiv anvendelse av kobling for kontrollformål vil innebære at man ikke tar teknikkens fordeler i bruk fullt ut. Til dette vil jeg innvende at man i såfall kun tar hensyn til fordeler som kan vinnes i et meget kortsiktig perspektiv. På lengre sikt er det etter min oppfatning nødvendig med fasthet å hevde det prinsipp at opplysninger som samles inn av en myndighet for et bestemt formål, ikke tillates anvendt for et annet formål, som publikum ikke har oversikt over. Uten dette prinsippet er risikoen stor for at vi får et ugjennomsiktig kontrollsamfunn som ingen av oss egentlig vil ha.

I min argumentasjon ovenfor har jeg tatt som utgangspunkt at det er mange hederlige samfunnsborgere som via koblingen havner urettmessig i nettet og tvinges til å bevise sin uskyld.

I en rettsstat er det imidlertid selvfølgelig at det ikke bare er de "hederlige" som har krav på retssikkerhetsgarantier. Også de som virkelig har gjort noe galt, har krav på visse garantier. Politi og påtalemyndighet må følge visse spilleregler overfor mistenkte personer. Etter min oppfatning er det i dag ting som tyder på at disse spillereglene uthules. Innen narkotikaetterforskning ser vi idag at det fremmes forslag om utvidede fullmakter til å drive telefonavlytting, og elektronisk avlytting av leiligheter mv. Veien er ikke lang fra dette til f. eks å gi politiet fullmakt til å undersøke bibliotekenes utlånsregistre for å sjekke hvem som har lånt bøker om dyrking av hasjplanter e.l. Eller for å ta et annet velkjent eksempel: Den norske oljemekleren Finn Malmberg ble funnet ved at politiet fikk opplysning om hvor han sist hadde benyttet sitt kredittkort.

Etter min oppfatning er det vel og bra at politi og påtalemyndighet, skattemyndigheter og trygdemyndigheter mv. får anledning til å benytte seg av den nye teknikken til å forebygge og oppklare ulovlige handlinger. Vi må imidlertid sørge for at det skjer på måter som ikke samtidig fører til en uthuling av rettssikkerhtsgarantiene, uten at vi egentlig er klar over hva som er i ferd med å skje. Et bærende prinsipp har vært at påtalemyndigheten har bevisbyrden for at en person er skyldig i straffbar handling. Med en etterhvert omfattende registrering av informasjon om hva personer til enhver tid foretar seg, er vi iferd med å havne i en situasjon hvor registrene sannsynliggjør bestemte handlinger (f. eks noe som ser ut som straffbare handlinger), slik at det er den enkelte som må bevise sin uskyld (Vi får en "omvendt bevisbyrde" med hensyn til straffbare handlinger.)

Det fremgår av argumentasjonen ovenfor at personvern inneholder flere av de samme elementer som de tradisjonelle rettssikkerhetsgarantiene. De utvides imidlertid noe, idet de får anvendelse også på områder der det ikke tidligere ikke har vært vanlig å bruke betegnelsen "rettssikkerhet."

Etter min oppfatning er det således fremdeles av største betydning at vi har et eget organ som har som hovedoppgave å forstå hva som er iferd med å skje: Et organ som kan forstå de prinsipielt viktige følgene for "personvernet" av nye registreringsformer og bruksmåter, og som har mulighet for å nå fram med sine synspunkter på en måte - og til et tidspunkt - som gjør at det blir hørt og tatt hensyn til. Datatilsynet har gjentagne ganger kunnet konstatere at de som skal løse en oppgave på et bestemt felt - eller som utreder mulige løsninger av en slik oppgave - ikke vurderer personverninteressene i tilstrekkelig grad.

2. TEKNOLOGISK UTVIKLING

2.1. Innledning - avgrensning

I utredningsoppdraget pkt. b), ble jeg bedt om å

"utrede hvilke problemer den betydelige utbredelsen av dataanlegg, spesielt mikromaskiner, kan ventes å medføre i de nærmeste år. Det gjelder både problemer knyttet til personvernet, og problemer knyttet til administrasjon av regelverket, så vel for Datatilsynet som for brukerne av EDB-anlegg"

Datatilsynet har store arbeidsoppgaver og begrensede ressurser. Av personregisterloven § 3 annet ledd punkt 1), fremgår det at Datatilsynet skal holde seg orientert om den generelle utvikling i bruken av personregistre og om de problemer som knytter seg til slike registre, samt sørge for informasjon i denne forbindelse.

Datatilsynet har - særlig på grunn av ressursmangel - ikke hatt mulighet for å gjøre systematisk arbeid med slik oppfølging. Det er imidlertid helt på det rene at den tekniske utvikling på dette området går så vidt fort, at bestemmelsene i personregisterloven på mange områder ikke lenger passer fullt ut. Videre skjer det en eksplosjonsartet utvikling i nye typer bruk av elektroniske hjelpemidler, som innebærer at det blir opprettet personregistre som biprodukter i annen virksomhet. Slike registre er i utgangspunktet konsesjonspliktige etter personregisterloven.

Jeg vil i det følgende først redegjøre for endel områder der den tekniske utvikling vil medføre en økende registrering av personopplysninger. For hvert område vil jeg påpeke enkelte problemer den någjeldende personregisterloven vil medføre for henholdsvis brukerne og for Datatilsynet. Dernest vil jeg drøfte om vedkommende form for registrering medfører vesentlige personvernproblemer.

Fremstillingen her tar først og fremst sikte på å påvise spesielle problemer på områder som kommer i tillegg til de ordinære "personregistre" som man tok sikte på å kontrollere da loven ble vedtatt i 1978. Det er grunn til å være klar over at de problemstillinger som lå til grunn da personregisterloven ble forberedt i 1970-årene nå kanskje er ennå mer aktuelle enn de var den gangen: Innen offentlig og private forvaltningsapparater skjer det en utstrakt innsamling, lagring og bruk av opplysninger om privatpersoner. Lagringskostnadene for informasjon har blitt drastisk redusert siden den gang, samtidig som programmer for fremfinning og kobling av informasjon har blitt langt mer effektive. Vi er inne i en utvikling, der alt som er registrert på EDB (eller skrevet på papir -

lest optisk inn på EDB) vil kunne søkes gjennom etter informasjon om bestemt person (se f.eks. nedenfor under avsnitt 2.8 om fritekst søkesystemer). Dette innebærer at rent teknisk sett, vil alt som er registrert om en person i mange forskjellige sammenheng, kunne sammenstilles (kobles). Det vil bare være et spørsmål om tilstrekkelige økonomiske interesser som står bak og er villige til å betale for en sammenstilling.

Fremstillingen her er underlagt klare begrensninger med hensyn til omfang og innhold. Dette følger av mandatet, og av den tid som har stått til rådighet. Jeg vil derfor konsentrere fremstillingen om visse av de mest fremtredende nye områdene som vil komme til å bety mye for personregisterloven og praktiseringen av den.

For enkelte av de bruksområdene for EDB som fremheves i det følgende, er det grunn til å understreke et moment som har betydning i tillegg til selve de tekniske mulighetene: De innebærer en skalaendring. Det er iferd med å bli introdusert en "forbrukerteknologi" (Teledata, "Elektroniske hjemmeterminaler", Elektronisk tekstbehandling, "bruksregistrering" osv.). Dette vil selvsagt medføre tilsvarende økning i problemene for Datatilsynet med å følge opp de reglene som skal gjelde for innsamling, lagring og bruk av personopplysninger.

Det har i norske teoretiske fremstillinger av personvern, vært vanlig å beskrive "personvernet" som den enkeltes interesse i best mulig herredømme over informasjon som beskriver ham/henne.

Denne interessen blir gjerne delt opp i flere andre interesser (jfr. nærmere om dette ovenfor under avsnitt 1.3.1). Således har vi interessen i:

- fullstendighet
- disktresjon
- å være opplyst
- borgervennlig administrasjon
- å unngå overdreven kontroll og uhjemlet maktbruk.

2.2. Elektronisk tekstbehandlingsutstyr - mikromaskiner

2.2.1. Utrustning - muligheter

Et område som skaper særlig problemer i forhold til personregisterloven, er den vide utbredelsen av

elektronisk tekstbehandlingsutstyr, og av forskjellige typer mikromaskiner. Mikrodatamaskinene er etterhvert så rimelige i anskaffelse, at de anskaffes for hobbybruk av privatpersoner. Slik personregisterloven er i dag, dekker den ikke privatpersoners opprettelse av personregistre. Dette er et særlig problem som jeg vil komme nærmere tilbake til nedenfor under avsnitt 4.2 i forbindelse med forslag til endring av § 1 i loven. Her vil jeg særlig ta for meg den stadig mer utstrakte utbredelsen av elektronisk tekstbehandlingsutstyr.

Det meste av det som skrives på elektronisk tekstbehandlingsutstyr med søkefunksjoner, og som inneholder personopplysninger (navn, fødselsnr., eller annen personidentifikasjon), vil være personregistre etter personregisterloven's definisjon. Det vil derved komme inn under reglene i personregisterloven.

Når man skriver dokumenter (brev, notater, referater, kontrakter, testamenter, etc.) på tekstbehandlingsutstyr, vil man som regel lagre det skrevne i en viss periode. Dokumentet er selvfølgelig lagret slik at det skal kunne finnes igjen. Dette foregår på den måten at operatøren gir dokumentet et "navn", som han/hun noterer seg eller husker, til det elektronisk lagrede dokumentet skal hentes fram igjen. Operatøren kan også hente frem den fullstendige listen over slike "navn" på dokumenter som vedkommende har lagret.

Operatøren vil ofte bruke personnavn som forekommer i teksten, eller som dokumentet har tilknytning til, som "navn" på dokumentet. I såfall vil vedkommende samling av dokumenter være et personregister i personregisterloven's forstand.

Hvis operatøren konsekvent ikke bruker personnavn som dokumentnavn, blir spørsmålet noe mer tvilsomt. Det finnes imidlertid endel tekstbehandlingsutstyr nå, som er slik at man kan søke på et hvilket som helst ord, som forekommer i en hvilken som helst tekst som er lagret. I såfall vil hele tekstmassen som til enhver tid er lagret i tilknytning til et slikt anlegg være et personregister (eller flere).

I mange av dem kan man (på tross av at de ikke har søking på "tvers" av dokumenter) søke seg fram til ethvert ord innen samme dokument. Ved en slik søking går pekeren på dataskjermen automatisk fram til første forekomst av søkeordet. Dernest kan man "bla" seg fram gjennom teksten til hver ny forekomst av ordet. Dersom det finnes navn på fysiske eller "juridiske" personer i noen av de tekstene som lagres, vil den lagrede teksten måtte anses for å være et personregister (eller en del av et personregister - avhengig av hvordan man trekker grensene for det enkelte register).

Opprettelse av slike "registre" innebærer som regel konsesjonsplikt etter § 9 i personregisterloven. Tekstbehandlingsfiler er som regel ikke av en slik art at de passer den beskrivelsen av "typeregistre" som er gitt

i forskriftene. De vil derfor sjelden omfattes av et av de unntak fra konsesjonsplikten som er oppstilt i forskriftene.

Mikromaskiner og elektronisk tekstbehandlingsutstyr er dessuten som regel utstyrt med en eller annen form for "arkiv"-system. Dette er programmer spesielt utformet for opprettelse av registre for gjenfinning av informasjon. Det må antas at registre av den typen saksbehandlere tidligere opprettet i form av små kortregistre, ringpermer alfabetisk ordnet osv., i fremtiden vil bli opprettet på mikromaskinene/tekstbehandlingsutstyret.

Elektronisk tekstbehandlingsutstyr vil i tiden framover bli tatt i bruk både i forvaltningen og i det private næringsliv i stadig økende utstrekning. Det er dessuten grunn til å tro at stadig flere vil gå til anskaffelse av slikt utstyr for privat bruk, idet prisene er iferd med å synke til rundt 10 000 kr. for relativt avansert utstyr.

Det utstyr som tas i bruk vil være av svært forskjellig kvalitet. Det vil spenne fra enkeltstående enbrukersystemer for "ren" tekstbehandling, til integrerte systemer for kontorautomasjon, som også omfatter tekstbehandling. Det er mye som tyder på at saksbehandlere og ledere selv vil sitte med utstyr på sin arbeidsplass, og at de vil bruke dette utstyret til bl.a. opprettelse av alt fra telefon- og adresselister, til presedensregistre og søkerlister ved ansettelse til stillinger.

2.2.2. ETB og problemer for registereierne

De som tar i bruk tekstbehandlingsutstyr vil sjelden tenke over at bruk av utstyret involverer en opprettelse av "registre" som er konsesjonspliktige etter personregisterloven.

Tekstbehandlingsutstyret vil dessuten oppfordre til en "ustrukturert" opprettelse av personregistre: Den enkelte tekstbehandlingsoperatør tar i bruk utstyret som hjelpemiddel til å holde styr på et personlig arkiv e.l.

Dersom de formelle krav som nå stilles i personregisterloven skulle tilfredsstilles, måtte det søkes konsesjon for hver enkelt type anvendelse av slikt utstyr, innenfor den enkelte bedrift/virksomhet. Dette medfører et voldsomt behov for informasjon internt i den enkelte bedrift/virksomhet, for å sikre at plikten overholdes. Selv med omfattende informasjon, er det høy sannsynlighet for at mange som strengt tatt er pliktige til å søke om konsesjon - av ren vanvare eller på grunn av forståelig villfarelse om de formelle kravene etter loven - ville unnlate å søke om konsesjon. Det er uheldig, og egnet til å bringe personregisterloven i vanry, å stille opp krav i loven som ikke kan følges opp i praksis.

Dersom "registereierne" (de som fører personregistre) fulgte opp lovens krav, er det utvilsomt at dette ville påføre dem et arbeid av relativt betydelig omfang med opplæring, diskusjoner med Datatilsynet, utfylling av søknadsskjemaer, og senere oppfølging av de konsesjoner Datatilsynet gir. Det er umulig å estimere kostnader på registereiernes hånd av dette arbeidet, men det kan umiddelbart fastslås at det vil dreie seg om betydelige beløp, dersom man ser alle brukere av tekstbehandlingsutstyr under ett.

2.2.3. ETB og problemer for Datatilsynet

Som jeg har vist ovenfor under avsnitt 2.2.1, vil nesten enhver bruk av selv det enkleste tekstbehandlingsutstyr innebære at det opprettes "personregistre" i personregisterlovens forstand. Personregisterloven, slik denne er utformet i dag, innebærer at slike "registre" stort sett vil være konsesjonspliktige. Nedenforunder avsnitt 3.7 - 3.8, og i avsnitt 4.5, vil jeg komme tilbake til Datatilsynets problemer med konsesjonsbehandling av de store mengder med mer tradisjonelt utformede registre. Konklusjonene der er basert på at konsesjonsordningen i forhold til dagens bemanning medfører for mye trivielt rutinearbeid. Dersom alle tekstbehandligsbrukere skulle søke konsesjon for det som formelt sett er personregistre i personregisterlovens forstand, ville dette rutinearbeidet mangedobles.

Tekstbehandlings-"arkiver" passer dårlig inn i de kategoriene med registre som er unntatt i forskrifter til personregisterloven. Ved konsesjonsbehandling kreves dessuten etter loven at det skal fastsettes hvilke typer opplysninger det er tillatt å ta inn i et personregister, og det må søkes om ny konsesjon for å endre dette. Tekstbehandlingsutstyret brukes til å opprette en type "registre" som meget vanskelig kan spesifiseres med hensyn til innhold. Det ville ofte bli behov for å endre konsesjoner. Datatilsynets arbeidsoppgaver ville bli mangedoblet i forhold til det som kommer inn av søknader i dag, dersom loven ble fulgt opp på dette punkt. Etter min oppfatning ville dette være svært uheldig for Datatilsynets arbeid med langt viktigere personvernoppgaver.

På den annen side er det også meget uheldig at denne meget store "registermassen" formelt sett omfattes av personregisterlovens konsesjonskrav mv. - uten at dette i det hele tatt følges opp i praksis. Dette er egnet til å bringe hele personregisterloven i vanry, med den følge at den blir oversett også på områder hvor det er viktig at prinsippene blir ivaretatt, og at det blir foretatt en reell kontroll av registrene.

2.2.4. Personvernproblemer - ETB

2.2.4.1. Generelt

Personregisterloven er i dag utformet slik at den ikke dekker privatpersoners innsamling, oppbevaring og lagring av personopplysninger. Som påpekt ovenfor vil privatpersoner i stadig økende grad ta i bruk det nye hjelpemidlet til rent private formål. Dette kan også komme til å skape personvernproblemer. Et spørsmål er derfor om man ikke allerede nå bør utforme lovgivningen slik at den i prinsippet også omfatter privatpersoners registrering av personopplysninger - i det minste med visse materielle regler.

2.2.4.2. ETB og interessen i fullstendighet

Tekstbehandlingssystemer kan brukes på mange forskjellige måter. Den mest vanlige vil likevel være at det benyttes til lagring og utskriving av tekster av forskjellige slag.

Det vil føre til meningsløse tilstander om man skulle kreve at den tekst som lagres på ETB skulle være "fullstendig." Man kan som eksempel tenke seg to advokater som fører en prosess mot hverandre, og som begge bruker ETB til å skrive og lagre prosesskrift. Skulle den ene kunne gå til motparten med personregisterloven i hånd og kreve at motparten sletter/endrer innholdet i sitt elektronisk lagrede prosesskrift?

Eller for å ta et annet eksempel: Datatilsynet har fått søknad om konsesjon for en "avisartikkelindeks". Med alminnelig kjennskap til fullstendighet og presisjonsnivå på mye av det som står i avisartikler som kan komme til å bli registrert i et slikt system, er det kan det fastslås at det vil være vanskelig å tilfredsstille personregisterloven´s krav til fullsendighet i et slikt register.

Man kan lage mange slike eksempler som viser hvor urimelig det ville være om forslag til vedtak, utkast til notater, rapporter, dokumentarlitteratur osv., ble utsatt for krav om retting eller supplering fra personer som er omtalt. Jeg finner det ikke nødvendig å utpensle dette nærmere.

Det samme utstyret som benyttes til ETB, kan imidlertid utmerket godt benyttes til å lage hva vi mer tradisjonelt har vært vant til å kalle registre. Således markedsføres mye av utstyret med såkalte "arkiv"- funksjoner, som innebærer at det er laget programmer som er spesielt utformet for å lette gjenfinning av dokumenter. Arkiver/registre som er bygget opp på denne måten, i den

hensikt å lette gjenfinning av informasjon om personer, faller klart innenfor det området personregisterloven er ment å skulle regulere. Det er imidlertid svært vanskelig å trekke noe klart skille mellom disse to anvendelsesmåtene. Overgangen mellom dem vil være glidende.

2.2.4.3. ETB og interessen i å være opplyst

Samme type problem oppstår i relasjon til innsynsrett etter loven § 7. Skulle f. eks en person kunne kreve innsyn i utkast til brev e.l. som ligger lagret på ETB, før det endelige brevet er utformet? Det gjelder ikke noe unntak for "interne dokumenter" e.l. etter personregisterloven§ 7, første ledd. Dette innebærer at forvaltningsorganer som tar i bruk ETB vil kunne oppleve at det gjøres en innsynsrett gjeldende overfor det som etter forvaltningsloven er kalt "interne dokumenter". Det unntaket for slike dokumenter som fremgår av § 7 annet ledd, siste punktum, gjelder bare overfor "opplysninger som ikke lagres eller bearbeides ved elektroniske hjelpemidler".

Forvaltningslovens regler om partsinnsikt kan kanskje påberopes for å hevde at det ikke gjelder innsyn i slike dokumenter. Jeg tviler imidlertid på at det ville være holdbart. Personregisterloven´s regler om innsyn i opplysninger lagret ved elektroniske hjelpemidler er av nyere dato, og de er utformet spesielt med sikte på elektronisk lagrede opplysninger. Spørsmålet om å ta med et slikt unntak i bestemmelsen er overveiet i forarbeidene og forkastet. Det heter således i Odelstingsproposisjon nr. 2 1977 - 78, s.57 sp. 1:

> "For såkalte manuelle registre forslår departementet derfor at unntaket for interne dokumenter etter forvaltningsloven § 18 skal gjelde tilsvarende. Når det gjelder EDB-registrerte opplysninger har departementet derimot ikke sett grunn til å gjøre noe slikt unntak. Det er særlig EDB-registrene krav om innsynsrett har tatt sikte på, slik at det kan være særlig grunn til å sikre innsynsretten her.(uthevet her). For øvrig fører økonomiske hensyn til at det er begrenset hva som blir EDB-registrert. Mengden av vurderingspregede uttalelser o.l. blir dermed i praksis mindre enn det som kan være tilfelle for manuelle registre."

Etter min oppfatning vil derfor personregisterloven´s innsynsbestemmelse gå foran de begrensninger i partsinnsiktsretten som er satt opp i forvaltningsloven §§ 18 og 19, i den utstrekning opplysninger lagres ved elektroniske hjelpemidler som f. eks. ETB. Jeg vil dessuten påpeke at den teknologiske utviklingen har ført til drastiske reduksjoner i lagringskostnadene siden Odelstingsproposisjon nr. 2 1977 - 78 ble skrevet - hvilket medfører at den siste delen av sitatet ovenfor er iferd med å bli helt misvisende.

Jeg behøver knapt si at dette vil skape store praktiske problemer. Noe av hensikten med ETB er f.eks at tekster raskt og lettvint skal kunne forandres. Den som begjærer innsyn vil aldri kunne forsikre seg om at den utskrift han/hun mottar er den samme som var lagret i maskinen på et bestemt tidspunkt. I tillegg kommer alle de vanlige innvendingene mot å gi innsyn i dokumenter som er på forberedelsesstadiet.

2.2.4.4. ETB og interessen i diskresjon

ETB skaper også spesielle problemer i forhold til interessen i diskresjon - selv om problemene på dette området ikke synes å være like stor som på de øvrige. Ett av de problem som oppstår, har særlig aktualitet for tekstbehandlingsanlegg med flere brukere. Det er vanskelig på slike anlegg å bygge opp en sikkerhet for at informasjon ikke kan hentes fram av andre enn de som er autorisert til det. Videre er det mye som tyder på at informasjon skrevet i brev, notater, betenkninger mv., og som tidligere ikke gikk inn i noe personregister, nå blir søkbar for kortere eller lengre perioder. Dette vil etter min oppfatning lett kunne føre til at noe som egentlig ikke var tiltenkt rollen som personregister, plutselig får nettop denne rollen. Hvis man f. eks har skrevet om en bestemt problemstilling og lagret det skrevne på ETB, kan man senere - når det dukker opp et bestemt problem - søke gjennom teksten ut ifra et hvilket som helst ord som kan tenkes å stå der, f.eks. navn. Vi får med andre ord lagret "personregistre" uten at det er tatt stilling til hva som bør lagres med sikte på fremtiden, og uten bevisste overveielser om hvorvidt det som skrives er egnet til bruk i fremtidige beslutninger.

I velstrukturerte og nøye planlagte EDB-systemer legges det ned betydelig arbeid for å sikre "datakvalitet". Rutiner for oppdatering av registre og sletting av uaktuell informasjon er en selvfølge, samtidig som det finnes avanserte metoder for maskinell kontroll med at informasjon er korrekt skrevet. I ETB-systemene er dette imidlertid ikke tilfelle. De er nettop utformet for å håndtere ustrukturert informasjon på en enklere måte enn tidligere. Samtidig spres dette utstyret i slike mengder at det nødvendigvis må bli en meget uoversiktlig flora av forskjellige "registre" som bygges opp rundt i bedrifter og på forvaltningens kontorer. På mange måter tror jeg at ETB-systemene vil overta den rollen som de private kortarkivene, presedensarkivene, ringpermene etc., har i dag.

Dette bildet kompliseres ytterligere av de såkalte "fritekst søkesystemene" (NOVA*STATUS, SIFT, STAIRS osv). Dette er EDB-programmer laget spesielt for å finne fram til informasjon som er lagret i ustrukturert form. Problemene forbundet med slike systemer er nærmere beskrevet nedenfor under avsnitt 2.8.

2.2.4.5. ETB og interessen i borgervennlig administrasjon

ETB tas i bruk ut fra effektiviseringsformål. I mange tilfelle fører bruk av slikt utstyr ikke bare til at man får gjort en bestemt jobb raskere og bedre, men at man får løst de primære oppgavene bedre fordi utstyret gir nye muligheter. Nettop den bruk av ETB som er beskrevet ovenfor, illustrerer dette. Man får ikke bare raskere og bedre maskinskriving og setting/redigering/forandring av teksten. I tillegg får man et EDB-registrert materiale som det kan søkes i på måter som ikke var mulige tidligere. Det synes innlysende at dette gir et grunnlag for en bedre oppgaveløsning. Brukt riktig vil derfor ETB etter min oppfatning kunne medføre fordeler, sett ut fra "interessen i en borgervennlig administrasjon."

Et aspekt som man imidlertid må ta i betraktning her, er det som noe diffust kalles for "samfunnets sårbarhet". Det jeg mener i denne sammenheng, er at den økende bruken av ETB medfører en økt avhengighet av dette hjelpemidlet til å løse oppgavene. Når hjelpemidlet settes ut av funksjon i kortere eller lengre perioder, vil det være vanskelig å betjene publikum tilfredsstillende.

2.2.4.6. ETB og interessen i å unngå overdreven kontroll

Som jeg har vært inne på tidligere innebærer den økte bruken av ETB at stadig mer informasjon lagres i såkalt "maskinlesbar form." Jeg ser dette som en klar fare, vurdert i lys av interessen i å unngå overdreven kontroll. Etter min oppfatning illustreres mitt poeng i denne sammenheng godt av de to eksemplene på bruk som er nevnt nedenfor under avsnitt 2.8 (dommer og avisstoff tilgjengelig i fritekst søkesystemer). Dersom all mulig slik informasjon gjøres søkbar, og gjøres tilgjengelig for forskjellige kontrollformål i privat virksomhet, eller i organer for stat og kommune, vil dette etter min oppfatning føre til uholdbare resultater.

2.3. Systemer for registrering av tjenestebruk

2.3.1. Utrustning - muligheter

Andre systemer som vil skape problemer i forbindelse med avgrensning i § 1 i personregisterloven, er systemer som innebærer en registrering av bruk av bestemte tjenester av forskjellig slag. Beslektede problemer oppstår ved innføring av moderne biblioteksystemer. I slike systemer vil det inngå personopplysninger, dels om forfattere av bestemte skrifter, dels om hvem som har lest hvilken informasjon. Videre har vi systemer for registrering av videoprogramutleie. Ytterligere en type systemer som synes å bli ganske utbredt, er telefonsentraler som

foretar registrering av hvilke numre det er ringt til, hvilke numre det er ringt fra, og lengden på telefonsamtaler. Teledata, tekst-TV, Telefax, Teletex og et utall av forskjellige informasjonssøkesystemer (f.eks Lovdatabasen, eller litteraturdatabaser), vil også inneholde visse opplysninger om hvem som har brukt vedkommende tjeneste, hvor lenge, og evt. også hva vedkommende har vist spesiell interesse for. For enkelhets skyld vil jeg i det følgende kalle slike systemer for "bruksregistre".

Felles for slike systemer er nettop at de foretar en automatisk registrering av personopplysninger for faktureringsformål. Siden slike personopplysninger skal benyttes til fakturering, tar jeg det for gitt at personregisterloven´s krav til systematikk i § 1 er tilfredsstillet slik at disse registrene faller inn under loven. Mange av dem vil derved også gå inn under unntaksbestemmelsene som er gitt i forskrifter vedrørende kunderegistre, og de vil være underlagt de betingelsene som gjelder for slike.

Samtidig vil denne faktureringsinformasjonen imidlertid under bestemte forutsetninger kunne brukes til å lage "interesseprofiler", eller "bekjentskapsprofiler" over brukerne i 7 systemet. Denne muligheten kan riktignok bare utnyttes av de som sitter sentralt i systemet. Det vil si de som kan skaffe seg adgang til systemets register over slik informasjon.

Det vi imidlertid må ta stilling til, er om det er ønskelig at samfunnsmedlemmene skal legge etter seg så mange "elektroniske spor" som kan lede til konklusjoner om deres gjøren og laden, som det i dagens situasjon ser ut til å ville bli. Informasjonen som svarer til disse sporene har vært registrert også tidligere, men gjenfinningsmulighetene og systematiseringsmulighetene har ikke vært de samme. Vi kan derfor si at det er noe helt nytt som er i ferd med å skje.

2.3.2. Bruksregistrering - problemer for registereierne

Med "registereierne" vil jeg i denne forbindelse mene de som er ansvarlige for vedkommende systemtype, og som derfor vil ha hånd om det personregister som opprettes. For slike registre, såvel som for ETB-registrene,vil det ofte være vanskelig å være oppmerksom på at registret reguleres av personregisterloven med forskrifter, og at det er underlagt begrensninger med hensyn til bruk. Som jeg vil komme tilbake til nedenfor under avsnitt 3.8, er kunnskapsnivået om personregisterloven svært dårlig, bl. a. på grunn av dårlig informasjon. Dessuten medfører de forskjellige nevnte systemene opprettelse av personregistre uten at brukerne egentlig er klar over, eller tenker nærmere over at det er dette som skjer. F. eks. vil alle "brukere" av et EDB-anlegg bli definert overfor EDB-anlegget som bruker. Dette innebærer at anlegget senere holder rede på hva denne brukeren har foretatt seg på anlegget, og det kan f.eks benyttes til å

belaste uttakskonto for maskintid etc. Relativt sjelden vil systemansvarlige personer tenke over at de egentlig har opprettet konsesjonspliktige personregistre, eller at slike opplysninger er underlagt personregisterlovens krav.

Dette innebærer en opplagt fare for at loven, slik den er i dag, vil skape svært mange lovovertredere. Som kjent anses det for å være uheldig med lovgivning som mange ikke tar hensyn til, og som det ikke finnes praktiske muligheter til å følge opp. I forhold til den typen registre som er beskrevet ovenfor, vil den gjeldende lovgivningen antakelig skape mange lovbrytere - enten fordi de ikke har kjennskap til lovens regler, eller fordi de kalkulerer oppdagelsesrisikoen som særdeles liten. Begge deler er opplagt uheldig.

2.3.3. Bruksregistrering - problemer for Datatilsynet

Det som i forrige avsnitt er angitt som problemer for registereierne, har sitt speilbilde i de problemer det skaper for kontroll og oppfølging av loven. Datatilsynet mister troverdighet ved å skulle håndheve et regelverk som på papiret gir god kontroll med utviklingen, men som ikke lar seg følge opp i praksis.

Dessuten vil denne registermengden bli så stor i årene som kommer, at arbeidsoppgavene med en grundig oppfølging og kontroll med slike registre vil bli en ennå mer uoverkommelig oppgave for Datatilsynet, enn oppfølging av de mer tradisjonelle personregistrene. Datatilsynet har etter min oppfatning hverken mulighet for å klare å holde seg ajour med teknikkens utvikling og muligheter, eller for å klare den rent praktiske arbeidsmengden ved henholdsvis forhåndskontroll (konsesjoner) eller etterhåndskontroll (inspeksjoner) av slike registre.

2.3.4. Personvernproblemer - bruksregistrering

2.3.4.1. Bruksregistrering og interessen i fullstendighet

De formene for registrering som er nevnt her, vil gi opplysninger om enkeltpersoners bruk av bestemte tjenester til bestemte tidpunkter. Sålenge opplysningene bare brukes til debitering av tjenestene, eller til å lage statistikk over tjenestebruk, skaper de forsåvidt ikke noe problemer i forhold til den enkeltes interesse i fullstendighet: De innsamlede opplysningene vil som regel være fullstendige nok sett i forhold til beslutninger om utsendelse av faktura mv., eller i forhold til en statistikk som tjenesteyteren stiller opp for sine interne planleggingsformål.

Hvis derimot opplysningene tas i bruk for andre formål, kan interessen i fullstendighet vanskeligere ivaretas.

Et eksempel kan illustrere dette. Dersom en bedrift innfører et telefondebiteringsutstyr for å kunne regnskapsføre reelle telefonutgifter på de respektive avdelinger, er dette i og for seg ikke noe problem. Hvis opplysningene derimot benyttes ukritisk til å vurdere om bestemte personer tar for mange private samtaler i arbeidstiden, er det behov for mer informasjon enn det som fremgår av telefondebiteringsutstyrets register. Problemet med slik tilleggsinformasjon er imidlertid at den ikke registreres i tilknytning til de enkelte samtalene som foretas. Senere vil det ikke være mulig å gjenskape tilleggsinformasjonen. Det som gjenstår er den nakne informasjon om oppringte numre og samtalens varighet. Det vil ikke stå noe om de bakenforliggende årsaker til at samtalene ble gjennomført.

Tilsvarende vil det ved bruk av kassaterminaler som automatisk registrerer antall anslag pr. tidsenhet for vedkommende terminaloperatør, vanskelig kunne treffes slutninger om hvor effektiv vedkommende operatør er. Betjeningen av en kassaterminal omfatter også det å behandle de kundene som står foran terminalen, hvilket innebærer faktorer som maskinen ikke kan registrere.

Det ville derfor etter min oppfatning være betenkelig å benytte slike registre til å treffe beslutninger rettet mot den enkelte, om lønn eller forfremmelse. Disse eksemplene er i og for seg relativt uskyldige, men vi kan tenke oss langt mer problematiske forhold, som f. eks i en "lekkasjesak" å bruke et telefondebiterings-register til å finne fram til hvem av de ansatte som har ringt til bestemte aviser, eller journalister - for eventuelt å gi synderen en reprimande, eller avskjed.

Det er etter min oppfatning ikke mulig å forlange at slike registre skal være fullstendige i forhold til alle mulige kontrollformål. Det kan også være betenkelig å kreve at de skal være det: Mange former for slik kontroll bør avvises på prinsippielt grunnlag.

Også her vil det etter min oppfatning være riktig å relatere innholdet til et bestemt formål - og nekte bruk av registrerte opplysninger for andre formål (se ovenfor under avsnitt 1.3.2).

2.3.4.2. Bruksregistrering og interessen i å være opplyst

Interessen i å være opplyst vil i mange tilfelle være oppfylt i forhold til slik bruksregistrering som jeg har beskrevet ovenfor - i ethvertfall til en viss grad. De fleste som benytter seg av en eller annen apparattype, der bruken skal belastes en eller annen konto, og som må identifisere seg for apparatet før bruk, vil vite at det foregår en registrering av bruken.

I mange tilfelle vil vedkommende imidlertid ikke vite om slik registrering uten at det gis uttrykkelig informasjon om hvilken registrering som foretas, og hva den skal

brukes til. Telefondebiteringsutstyr innstallert på en arbeidsplass eller på et hotellrom, er et godt eksempel på dette. Den enkelte trenger ikke selv oppgi noen form for identifikasjon overfor systemet, idet vedkommende er identifisert gjennom sin tilknytning til vedkommende kontorplass eller hotellrom der telefonapparatet befinner seg. Den enkelte vil da ikke få noe varselsignal om at det foregår en registrering, eller om hva en slik registrering skal brukes til.

Brukt for rene debiteringsformål må slik informasjon sies å være harmløs - særlig sålenge apparatbrukerne gjøres uttrykkelig oppmerksom på den bruk som foregår. (For telefondebiteringsutstyr er det i dag oppstilt et krav om at apparatene skal påklebes et merke som uttrykkelig gjør oppmerksom på hvilken registrering som foregår).

Ingen vil vel egentlig bestride "apparateierens" rett til å registrere opplysninger som er nødvendige for å utstede en korrekt regning til den som har benyttet apparatet, eller til å lage statistiske sammenstillinger over bruk. Normalt vil personen være informert om dette og gi sitt stilltiende eller uttrykkelige samtykke til en slik registrering og bruk.

Når denne informasjonen derimot tas i bruk for helt andre formål enn debitering - som f. eks. etterforskning eller kontroll - vil dette ofte være godt utenfor det den enkelte har kjennskap til. Disse systemene vil derfor skape betydelige problemer sett i forhold til ivaretakelse av interessen i å være opplyst. Etter min oppfatning bør interessen i å være informert i disse tilfellene også omfatte det å være informert om hva den registrerte informasjonen kan brukes til (hva det er tillatt å bruke den til). Dette innebærer et krav om at informasjonen bare skal kunne brukes for det formål den opprinnelig ble registrert for, og som den enkelte har samtykket i, og at vedkommende må forespørres før det foretas endringer i bruken. En slik forespørring vil vel imidlertid i forhold til etterforskning og kontroll gi liten realistisk beskyttelse for enkeltpersonen. Om vedkommende ikke har vært mistenkt for å ha gjort noe galt før en slik forespørsel blir gjort, vil han/hun iallefall være det etter, dersom svaret er negativt.

2.3.4.3. Bruksregistrering og interessen i diskresjon.

De langt fleste bruksregistreringssystemer har til nå vært relativt uoversiktlige systemer, der det ikke har vært mulig å lage spesielle "bruksprofiler" over de som er registrert. Med de moderne bruksregistreringssystemene er dette i ferd med å endre seg radikalt. "Elektroniske spor" som gir oversikt over hva folk foretar seg til forskjellige tidspunkter, kan brukes til å sannsynliggjøre at vedkommende har foretatt seg noe "ulovlig". Informasjonen i EDB-systemene om bestemt bruk, vil imidlertid fremstå som objektiv registrering av bruk, som den enkelte i ettertid vil ha vanskelig for å motbevise - simpelthen fordi den enkelte ikke foretar

noen tilsvarende detaljert registrering av sine egne handlinger.

Etter min oppfatning vil det derfor klart innebære en trussel mot interessen i diskresjon, hvis slike opplysninger kommer på avveie, og/eller brukes til beslutninger som går ut over den enkelte.

2.3.4.4. Bruksregistrering og interessen i borgervennlig administrasjon

Automatisk bruksregistrering tas i bruk på mange felt. Ett av formålene vil ofte være å tilby bedre og mer detaljert informasjon om hvilken bruk som er foretatt (spesifisert regning fra televerket etc.). For den som i etterhånd er interessert i å kontrollere om regningen er korrekt, er slike former for registrering en fordel. Vi vil vel si at vedkommende får bedre tjenester, og at administrasjonen som yter tjenestene er bedre istand til å fylle behovet for informasjon.

En forutsetning for at dette skal være tilfelle, vil det være at det som registreres, og som personen mottar som informasjon om forbruk, er informativt. Vi kjenner alle til de mer eller mindre uforståelige remsene med utskrift fra EDB-systemer, som nærmest forutsetter at man har satt seg grundig inn i systemdokumentasjonen for at man skal forstå dem. Jeg forutsetter imidlertid at utskriftene har en form som gjør dem fortåelige. Under denne forutsetningen mener jeg at bruksregistreringssystemene etter sitt formål vil gi nyttig informasjon til brukerne av systemene. De vil derfor være med å tilfredsstille interessen i en "borgervennlig" administrasjon.

2.3.4.5. Bruksregistrering og interessen i å unngå overdreven kontroll

De stadig mer utbredte bruksregistreringssystemene vil føre til at det lagres stadig flere "elektroniske spor" som kan bidra til å danne bilder av hva et menneske har foretatt seg. Dette er imidlertid en ren mekanisk registrering av hendelser. Det foretas ikke samtidig noen registrering av årsakene til den handlingen som det registreres noe om. Menneskenes hukommelse er høyst mangelfull. De går ikke rundt og husker i detalj hva som er årsaken til bestemte handlinger, som f. eks hvorfor de ringte et bestemt telefonnr. en bestemt dag. Bruksregistreringssystemene vil imidlertid foreta en nitid registrering av faktiske hendelser. Dersom disse benyttes til andre formål enn å fakturere faktisk bruk, lage statistikk etc. kan informasjonen være misvisende for formålet. Jeg anser bruksregistreringssystemene for å være en av de mest alvorlige truslene mot interessen i å unngå overdreven kontroll, nettop fordi de innebærer en omfattende lagring av "elektroniske spor", som kan benyttes til å lage oversikter over hva et menneske har foretatt seg i et bestemt tidsrom.

2.4. Elektronisk post og TELEDOC-systemer

2.4.1. Utrustning - muligheter

Innen kontorautomatisering arbeides det mye med å utvikle EDB-systemer som skal kunne brukes til å utveksle meldinger, og til å arrangere "møter" basert på geografisk spredt beliggende EDB-terminaler. Slike systemer har fått mange forskjellige navn, avhengig av hvilket bruksområde de er utformet for, og hvem de skal betjene. Telekonferanser, datamaskinassistert tekstkommunikasjon, elektroniske meldingsformidlingssystemer, og elektronisk post, er alle forskjellige varianter av denne typen system. Disse systemene benevnes i en artikkel av Peter Seipel som "TELEDOC" ("TELEDOC and open records", Peter Seipel. Artikkelen vil bli publisert i en kommende spesialutgave av Computer Law Journal, som handler om "Computer Law policy").

I tillegg til å innebære en bruksregistrering av samme type som jeg har behandlet foran under avsnitt 2.3, vil disse systemene også inneholde meningsytringer avgitt av deltakerne. Disse meningsytringene vil etter min oppfatning ha samme krav på beskyttelse mot uvedkommendes innsyn og bruk, som vanlige brev har det. Slike systemer reiser en rekke problemer i forhold til vanlig straffelovgivning, i forhold til alminnelige kjøpsrettslige regler om tilbud og aksept av tilbud, i forhold til reglene om offentlighet av forvaltningens "dokumenter" osv.

De vil etter min oppfatning reise alvorlige personvernproblemer også. Via slike systemer vil de som er tilknyttet kunne utveksle informasjon på samme måte som man i dag gjør det pr. brev eller telefon. I tillegg inneholder systemene muligheter for å arrangere "konferanser" med et stort antall deltakere, som ikke trenger være samtidig tilstede ved sine terminaler. Systemet administrerer bidragene og kommentarene fra deltakerne og holder oversikt over hvem som har deltatt i hva. Slike systemer er også velegnet til samarbeid mellom flere personer om utarbeidelse av rapporter, bøker osv. De kan benyttes til meningsmålinger, avstemninger, forespørsler til en vid krets av personer, annonsering, og melding av forskjellige forhold.

TELEDOC-systemer kan med fordel kombineres med andre EDB-systemer, som f.eks tekstredigering, tekstsøking, planlegging og statistikk.

TELEDOC-systemer er i ferd med å få en meget stor utbredelse. Det finnes flere internasjonale systemer som er åpne for abonnenter. Et enkelt av disse håndterer omkring 25 millioner meldinger pr. år (Raymond R Panks, The EMS Revolution. Computerworld 14 (1980) No 34 ("In

Depth" article)). Det pågår dessuten for tiden omfattende arbeid innen mikromaskinutviklingen for å finne fram til standardiserte måter for kommunikasjon mellom flere mikromaskiner. Dette vil føre til at mikromaskiner kan knyttes sammen som "elektroniske postkasser" i omfattende nettverk. Mikromaskiner med kommunikasjonsenheter kan man nå få til en pris under kr. 20 000. De vil synke ytterligere i pris, og de vil få en betydelig utbredelse etterhvert som flere mennesker blir fortrolige med bruken av dem. Det er derfor all grunn til å vurdere forskjellige sider ved slike systemer ut fra rettslige synspunkter.

2.4.2. Elektronisk post - problemer for registereierne

Som nevnt foran betegner "registereierne" her de som er ansvarlig for opprettelse og drift av systemene.

I forhold til den någjeldende personregisterlovgivning medfører slike systemer opprettelse av flere registre. På samme måte som ved ETB-systemene innebærer elektronisk post opprettelse av registre for fakturering sformål, som også vil kunne innebære en registrering av meninger og særlige interesser hos de som benytter systemet. Slike systemer vil imidlertid være organisert på måter som skiller seg fra det man vanligvis assosierer med begrepet "register". Ikke desto mindre vil de omfattes av personregisterlovens registerbegrep, og på grunn av systemenes manglende standardisering mht. innhold, formål og bruksområde, vil det ikke være mulig å regulere slike registre ved forskrifter etter oppskriften i personregisterloven § 9. De må derfor undergis individuell konsesjonsbehandling.

I mange tilfelle må man dessuten gå til det skritt å gi forskjellige konsesjonsvilkår for flere typer ulik bruk av det samme systemet. Etter personregisterlovens system er det den som oppretter et register som har ansvaret for å søke om konsesjon mv. TELEDOC-systemene vil for en stor del bli stillet til rådighet av leverandører av datatjenester - f.eks. en datasentral. På datasentralens hånd opprettes visse registre for fakturering formål, og visse registre som viser tilknytning mellom to eller flere terminaler tilknyttet samme "konferanse" (serie av meningsutvekslinger via systemet). Videre vil det på datasentralens hånd være "registre" som viser hva en person har ytret i en bestemt sammenheng.

Ikke desto mindre vil det være kundene hos datasentralen som knytter forbindelse og som har hånd om hvem som skal kunne få være med i en bestemt "konferanse", og som avgjør hva som skal bli "registrert" i systemet. Dette reiser vanskelige problemer i forhold til personregisterloven slik denne er utformet i dag. Loven er i dag utformet med tanke på velstrukturerte "registre" i tradisjonell forstand, som er opprettet av en organisjon for et bestemt formål.

TELEDOC-"registerne" er ustrukturerte, og de som stiller apparatet til rådighet, og som på en måte "fører" registerne, har ikke rådighet over innholdet i dem i det hele tatt.

Heller ikke noen enkelt deltaker vil imidlertid ha rådighet over den totale mengden med innlegg i en bestemt konferanse. Et nærliggende spørsmål (som det ville føre for langt å diskutere nærmere her) er hvem som er "eier" av inleggene i en slik konferanse.

2.4.3. Elektronisk post - problemer for Datatilsynet

Heller ikke overfor systemer for elektronisk post vil personregisterloven gi noen tilfredsstillende reguleringsform. Datatilsynets muligheter for oppfølging overfor de som fører "registerne" vil også her være svært vanskelig, idet registeransvaret ikke vil kunne plasseres hos noen bestemt: registeret utvikler seg gradvis etterhvert som det sendes meldinger i systemet, og den som stiller systemet til rådighet vil ha liten innflytelse på innholdet i "registeret". Dette kan muligens dekkes opp i klare avtaler med de som får adgang til å knytte seg til slike systemer, men jeg tviler på om dette vil gi noen egentlig tilfredsstillende løsning på problemene. Datatilsynet vil stadig ha alvorlige problemer med å utforme konsesjoner/forskrifter for slike registre ut fra personregisterloven slik den er utformet i dag.

I databehandlingsbransjen ventes slike systemer å få en betydelig utbredelse i årene som kommer. Systemene vil ikke bare være basert på at flere brukere er tilknyttet samme store maskinsentral: Vi vil få en stadig økende utbredelse av småmaskiner som kan kommunisere med hverandre via det offentlige datanettet. Dette vil ytterligere bidra til pulverisering av "register"-begrepet, og av registeransvaret. Dette vil skape betydelige problemer for Datatilsynet både fordi det blir meget vanskelig å plassere ansvar og fastsette adekvate regler i konsesjoner, og fordi det kommer til å bli et meget stort antall slike "registre".

Som jeg kommer tilbake til nedenfor under avsnitt 2.4.2, vil slike systemer dessuten skape betydelige problemer i forhold til personregisterloven § 7 om innsynsrett. Dette vil påføre Datatilsynet betydelig merarbeid på grunn av et ikke ubetydelig antall søknader om unntak fra innsynsrett for opplysninger lagret i slike systemer, og som har karakter av å være "interne notater" osv. Slike søknader vil kreve et grundig og omfattende saksbehandlingsarbeide fra Datatilsynets side, og beslutningene vil neppe kunne standardiseres i særlig grad.

2.4.4. Personvernproblemer - elektronisk post

2.4.4.1. Elektronisk post og interessen i fullstendighet

Ovenfor under avsnitt 2.3.4 er personvernproblemer ved bruksregistrering tatt opp. Siden TELEDOC-systemene må holde et nøyaktig regnskap med hvem som er autorisert til å lese hvilke meldinger, og hvilke meldinger den enkelte rent faktisk har lest, er de nødt til å ha nokså avanserte bruksregistreringssystemer. Det som er sagt om slike systemer foran under avsnitt 2.3.4, får derfor fullt ut anvendelse også overfor TELEDOC-systemene.

Her vil jeg imidlertid se litt på den informasjon som utgjøres av selve meldingene i systemet. Slike meldinger kan inneholde informasjon om nær sagt hva som helst. De kan bestå av artikler om politiske, religiøse eller faglige spørsmål. De kan inneholde forespørsler av forskjellig slag, og de kan inneholde diskusjonsinnlegg i debatter om forskjellige emner. De kan benyttes til stemmegivning, til meningsmålinger, og til bestilling av varer og tjenester. Det er dessuten grunn til å tro at slike systemer vil bli gjenstand for markedsundersøkelser, og forskjellig former for forskning for å finne ut hvem som benytter dem, og til hvilke formål de benyttes.

Så lenge informasjonen i slike systemer benyttes etter sitt formål, vil den kunne fremstå som fullstendig, fordi den benyttes i en bestemt sammmenheng, og beregnet på et bestemt publikum. Dersom slik informasjon imidlertid løsrives fra sin sammenheng, eller gjøres kjent for et annet publikum enn den er beregnet for, vil den kunne gi et meget misvisende inntrykk. Beslutninger (inkludert sosiale reaksjoner) på grunnlag av slike ufullstendige opplysninger, vil selvfølgelig lett kunne bli gale.

2.4.4.2. Elektronisk post og interessen i å være opplyst

Interessen i å være opplyst, vil oftest være oppfylt i forhold til ordinær bruk av TELEDOC-systemene. Det er den enkelte selv som skriver inn informasjonen i systemet (når vi ser bort fra "bruksregistrering", som foregår automatisk) - og ut ifra sitt kjennskap til systemet vil vedkommende vite hvordan informasjonen blir brukt. I slike tilfelle vil interessen i å være opplyst stort sett være tilfredsstillet.

Jeg vil imidlertid advare sterkt mot at slike systemer skal kunne tas i bruk for andre formål enn de som brukerne kjenner til. Bl.a. må det sikres at informasjonen i meldingene ("brevene") i systemene er tilstrekkelig beskyttet mot lesing av andre enn de som de er beregnet på. Bruksstatistikker mv. må være beskyttet ved anonymisering osv. Det må sørges for at det blir

etablert tilstrekkelige rettssikkerhetsgarantier mot politietterforskning, overvåking el., overfor bruk av systemene.

Slike systemer kan imidlertid også benyttes til å skrive noe om tredjepersoner. Disse tredjepersonene vil ikke vite om hva som foregår. Et eksempel på slik bruk av systemene vil vi f. eks ha når de blir tatt i bruk i ansettelsessaker, eller til andre personaladministrative formål. Systemer av denne typen vil være velegnet til å utføre saksbehandling i flere ledd, og det vil være fritt spillerom for brukerne av systemet til å skrive inn sine oppfatninger og vurderinger av personer som skal innstilles til ansettelse i en stilling, til forfremmelse o.l. Vi kan tenke oss en rekke andre måter for bruk av slike systemer som også vil innebære at det informeres om tredjeperson.

Vi har i forvaltningsloven egne regler om partsinnsikt. I offentlighetsloven har vi egne regler om offentlighet av forvaltningens dokumenter. Disse reglene inneholder bl.a. en rett til å se over forvaltningens journaler. Journalene vil være et viktig hjelpemiddel for å finne fram til dokumenter som inneholder informasjon en er interessert i å studere nærmere - også dokumenter om en selv.

Forvaltningslovens regler vedrører imidlertid dokumenter i tradisjonell forstand, skrevet på papir. Offentlighetsloven er foreløpig blitt tolket slik at den ikke gjelder for EDB-lagret materiale (Her har det imidlertid ved den nylig vedtatte revisjon av offentlighetsloven blitt åpnet en hjemmel til å regulere spørsmålet i forskrifter. Slike forskrifter er ennå ikke gitt). Det samme vil antakelig gjelde i forhold til forvaltningslovens regler om partsinnsikt. I den utstrekning TELEDOC-systemer tar over for dokumenter i form av papir, vil de rettigheter som er gitt den enkelte i form av partsinnsikt, innsyn i journaler mv. bli uthulet.

På den annen side vil den enkelte ha en innsynsrett etter personregisterloven § 7 i slike systemer. Den enkelte vil vel imidlertid neppe ha tilstrekkelig oversikt til å vite hva han eller hun skal be om å få se. De samme problemer i forhold til innsyn i interne dokumenter m.v. som nevnt ovenfor under avsnitt 2.2.4.3 i tilknytning til ETB, vil imidlertid gjøre seg gjeldende også overfor TELEDOC-systemene. Dette vil etter min oppfatning skape betydelige problemer ved praktisering av reglene. Slik personregisterloven er i dag, må den enkelte registereier søke om unntak fra innsynsrett i slike registre i hvert enkelt tilfelle, i medhold av personregisterloven§ 7, femte ledd.

2.4.4.3. Elektronisk post og interessen i diskresjon

De som tilbyr store kommersielle systemer for elektronisk post, som skal konkurrere med de tradisjonelle tjenestene

til Postverk og Televerk, er nødt til å legge betydelige anstrengelser i sikring av "dokumentene" i systemene mot uautorisert lesing. Et tradisjonelt brev sendes normalt i lukket konvolutt, og brevbrudd er forbudt og straffbart. Det samme gjelder nå etter endring i brevbruddparagrafen i Strl. antakelig overfor EDB-lagrede "brev", jfr. strl § 145. Dette gir antakelig en brukbar formell beskyttelse av interessen i diskresjon for slike meldinger. Også denne systemtypen bidrar imidlertid til å skape en rekke - tildels ganske markerte - "elektroniske spor" etter de som bruker systemene. Slike spor finnes ikke på samme måte etter brev som har vandret fra en avsender til en mottaker - medmindre det foreligger en plikt til å bevare kopi av brevet, og en plikt til å ha fortegnelser over alle brev (som f. eks i forvaltningen). Den viktigste forskjellen i forhold til tradisjonell post ligger likevel i det faktum at selve brevets innhold til enhver tid ligger registrert i systemet, sålenge det ikke er slettet. Det vil med andre ord foreligge en teknisk mulighet for å lese innholdet i brevet. Det blir derfor sentralt å finne ut hvordan man skal skape tilsvarende sikkerhet og rettssikkerhetsgarantier rundt et elektronisk "brev", som rundt et vanlig papirbrev. Videre er det viktig å skape tilsvarende holdninger overfor "brevbrudd" på elektroniske brev, som vi forøvrig har opparbeidet gjennom flere århundre overfor ordinære brevbrudd.

En videre utbredelse av TELEDOC-systemer uten slik sikkerhet, slike garantier, og klare holdninger til overtredelse, vil etter min oppfatning innebære alvorlige trusler mot interessen i diskresjon.

2.4.4.4. Elektronisk post og interessen i borgervennlig administrasjon

Det er vanskelig å bedømme om TELEDOC-systemene vil fremme en "borgervennlig administrasjon". Også slike systemer tas i bruk ut ifra effektiviseringsbetraktninger, og det vil vel som regel inngå i slike betraktninger at publikumsservicen skal bedres, eller i det minste ikke forverres. Hvorvidt slike systemer vil bidra til en mer borgervennlig administrasjon, vil antakelig avhenge av hvordan systemene tas i bruk.

Forutsatt at man skaper samme (eller helst bedre) muligheter til oversiktlighet over hva som foregår innen administrasjonen som når man benytter papirsystemer, vil jeg rent umiddelbart tro at bedrede kommunikasjonsmuligheter innen administrasjonen skulle kunne gjøre den mer "borgervennlig".

Samme reservasjon med hensyn til sårbarhet overfor systemer ute av funksjon gjør seg imidlertid gjeldende for TELEDOC, som jeg ovenfor har nevnt i forbindelse med elektronisk tekstbehandling (ETB): En økende bruk av TELEDOC-systemer som kommunikasjonsmiddel mellom forskjellige deler av offentlig og privat administrasjon,

vil medføre en avhengighet. Når dette kommunikasjonsmiddelet settes ut av funksjon i kortere eller lengre perioder, vil det (medmindre det er tatt tilstrekkelige forholdsregler) være vanskeligere å betjene publikum tilfredsstillende.

2.4.4.5. TELEDOC og interessen i å unngå overdreven kontroll

Vanlige brev setter ikke spor etter seg, og de er fysisk utformet slik at det stort sett er mulig å se om noen har tilegnet seg kunnskap om innholdet i dem. Derfor er det relativt uproblematisk å sende vanlige brev. Det er etablert klare grenser for hva politi og andre kontrollmyndigheter kan gjøre med dem, og for hvordan de må gå fram for å få adgang til innholdet.

Som nevnt foran finnes det ikke slike klare, etablerte mekanismer i forhold til TELEDOC og andre elektroniske systemer. Dessuten vil disse systemene inneholde selve innholdet i "brevet" uten at det er fysisk pakket inn på noen måte. Riktignok kan det pakkes inn i "logisk" forstand, ved EDB-tekniske sikringstiltak av forskjellig slag. Det vil imidlertid være mye vanskeligere for den som er en "dum" bruker av TELEDOC-systemet å kunne konstatere om noen har tilegnet seg kunnskap om brevets innhold. TELEDOC vil derfor etter min oppfatning være en type systemer som innebærer en mulighet for å kontrollere, fordi systemene fører til at det opprettes "elektroniske spor" som en kontrollmyndighet kan ha interesse av. Hittil har slike systemer kanskje i særlig grad blitt tatt i bruk i universitets- og forskningsmiljøer. I krigs- og krisesituasjoner vil slike miljøer ofte være utsatt for spesiell oppmerksomhet. TELEDOC-systemene vil - dersom de får utstrakt anvendelse, gi verdifull informasjon om holdninger og synspunkter hos brukerne, og om hvilke personer som står i kontakt med hverandre via systemet.

Et nærliggende spørsmål, er om vi ville finne oss i et pålegg om at kopi av alle brev vi skriver skulle oppbevares i en viss tid hos postverket, sammen med navn og adresse på avsender og mottaker. Dette ville være helt utenkelig, på samme måte som det ville være utenkelig at innholdet i telefonsamtaler ble registrert på lydbånd, sammen med navn og adresse (eller telefonnr.) på den vi har ført samtalen med.

Dette er spørsmål som etter min oppfatning bør tas i betraktning i forbindelse med den utvikling av nye kommunikasjonstjenester som nå foregår i stadig økende tempo.

2.5. Betalingsformidling - salgspunktterminaler

2.5.1. Utrustning - muligheter

Vi står nå på terskelen til et "kontantløst" samfunn, der finansielle verdier og tilknyttede data blir overført elektronisk, ved hjelp av EDB. Systemer for elektronisk betalingsformidling, og for elektronisk registrering av verdipapirer er allerede i full drift i samfunnet rundt oss.

Det finnes mange forskjellige typer slike systemer. En utførlig beskrivelse av EDB i betalingsformidlingen, er gitt i NOU 1977:56 "Databehandling i betalingsformidlingen". Jeg har fått bekreftet på bankhold at selv om denne utredningen er 5 år gammel, er hovedlinjene og de tekniske beskrivelsene fremdeles gyldige.

Viktigst sett ut fra personvernsynspunkt i den utviklingen som er beskrevet, er det etter min oppfatning at vi også i betalingsformidlingen vil få en økende registrering av transaksjonsopplysninger - både innenfor betalingsformidlingsinstitusjonene, og innenfor detaljhandelen.

De såkalte salgspunktterminalene er ikke særlig utbredt ennå. Mange regner imidlertid med at nettop varehandelen vil være det neste store marked som åpner seg for leverandører av EDB-utrustning (etter kontorsektoren, som åpnet seg for et par år siden). Det foregår nå i økende grad en merking av dagligvarer med EAN-strekkoder (European Article Number), som ved hjelp av optisk leseutstyr gjør det mulig å lese av den enkelte artikkels varenummer i kassen i butikken (i stedet for at kassaoperatøren taster inn prisen på vedkommende vare). Den optiske leseren står i forbindelse med en datamaskin, som har lagret opplysninger om varens pris etc. Disse opplysningene skrives ut på kvitteringen, som normalt vil inneholde flere opplysninger enn en vanlig kassalapp (f. eks. varetype, mengde og pris). Samtidig brukes opplysningene til å generere statistikk- og styringsdata for butikken (lagerstyring, oversikt over varebeholdning, regnskapsdata osv.). Det er vanlig å regne med at minst 80 % av varene må være merket med koden for at det skal være lønnsomt å benytte slikt utstyr. Foreløpig ligger merkingen av varer på det norske marked langt under dette, men det foregår stadig en økning.

Samtidig fører den alminnelige pris/ytelsesforbedringen innenfor EDB-bransjen til at det nødvendige utstyret blir stadig billigere og bedre.

Parallellt med dette foregår det en utvikling innenfor betalingsformidlingen, som innebærer at den enkelte kunde kan benytte sitt betalingskort som betalingsmiddel i butikkassen (slike eksperimenter foregår også Norge). Denne kan stå i direkte forbindelse med en betalingsinstitusjon, som automatisk overfører (eller besørger overført - via en såkalt "clearing-sentral") det aktuelle beløp fra kundens konto til forretningens. Det eksperimenteres flere steder i utlandet også med å

tillegge vanlige forretningskasser funksjoner, som tidligere normalt måtte utføres i banken, som f.eks innskudd og uttak av penger fra konto, betaling av regninger osv.

Dette innebærer at den enkelte vil legge etter seg en rekke elektroniske spor som sier noe om hvor vedkommende har oppholdt seg på bestemte tidspunkter, og hva vedkommende har tatt ut av kontanter eller har kjøpt. Slike opplysninger er nødvendige for revisjons- og kontrollformål internt i betalingsinstitusjonen, og i forretningen. Disse opplysningene vil bli mer detaljerte enn hva som har vært vanlig tidligere, og det vil kunne lages en langt mer fullstendig oversikt over den enkeltes forbruk og økonomiske disposisjoner. Få vil vel reagere på om opplysningene brukes til statistikker, revisjons- og kontrollformål.

Samtidig vil imidlertid opplysningene kunne si noe om kontoinnehaverens forbruksvaner, reisemønster osv. Når de bli detaljerte nok, kan de gi nyttige indikasjoner for politi og skattevesen om samsvar mellom forbruk og inntekt, om økonomiske forbindelser mellom forskjellige personer, mv. Slik informasjon vil også kunne brukes i markedsundersøkelsesøyemed, og som grunnlag for selektiv markedsføring.

Et eksempel fra USA (beskrevet i tidsskriftet "Privacy Journal", oktober 1981, Vol. VII, no.12), viser hvilke muligheter som er innebygget i de moderne salgspunktterminalene, som i fremtiden vil bli å finne i supermarkedene. Et markedsundersøkelsesfirma utnytter en kombinasjon av kabel-TV, salgspunktterminaler og EDB. Undersøkelsen innebærer at familiens "hovedinnkjøper" gir endel sentral informasjon til firmaet, så som inntekt, antall barn, boligforhold, kjæledyr og andre personlige opplysninger. Vedkommende blir forsynt med et identifikasjonskort, som skal presenteres hver gang han/hun handler i en butikk som er utstyrt med salgspunktterminal (denne registrerer hvilke varer som er kjøpt og hva de koster). Kunden får også en "sort boks" til å sette på sitt TV-apparat, og som bevirker at apparatet kan motta spesielle signaler kun beregnet på deltakerne i undersøkelsen. Undersøkelsesfirmaet sender ut egenproduserte reklameinnslag til deltakerne, som ikke vet hvilke reklameinnslag som går til alle, og hvilke som er en del av undersøkelsen. Undersøkelsesfirmaet registrerer imidlertid opplysninger om dette sammen med opplysninger om hva forsøkspersonene kjøper på sine påfølgende handlerunder i butikkene. Dette gjør det mulig å drive markedsføringsforskning på måter som ikke var mulig tidligere, og det synes nærliggende å påpeke mulighetene ordningen åpner for manipulering med forbrukerne, dersom slike forsøk senere skulle bli gjennomført <u>uten</u> informert samtykke fra deltakerne i undersøkelsen.

Kombinasjonen salgspunktterminaler som foretar en detaljert registrering av hva som kjøpes, og elektronisk betalingsformidling der det foretas en nøyaktig

registrering av hvem som betaler for det enkelte salg, innebærer at tilstrekkelig informasjon registreres til å gjennomføre undersøkelser som tilsvarer den ovenfor nevnte.

2.5.2. Elektronisk betalingsformidling - problemer for registereierne

Registereierne vil i denne sammenheng delvis være den enkelte butikk eller butikk-kjede, delvis betalingsformidlingsinstitusjonen. Systemer av den typen jeg har skissert ovenfor, medfører opprettelse av personregistre i personregisterlovens forstand. Dels vil de falle inn under det som nå er regulert i forskriftene til personregisterloven som "kunderegistre", og dels vil de falle inn under "kunderegister i bank". De någjeldende forskriftene kan muligens dekke integrasjonen mellom betalingsformidlings- og salgspunktsystemene. Det er imidlertid sannsynlig at særlig reglene om bankenes kunderegistre vil passe relativt dårlig for en systemløsning der kassererpersonale i institusjoner utenfor banken vil ha tilgang til visse opplysninger om bankens kunder.

Et særlig problem vil det være at utstyret spres utover til en rekke brukere som vil ha små kunnskaper om personregisterloven og om forskriftene til denne. Dette medfører krav om en betydelig informasjonsinnsats for at reglene skal bli fulgt opp. Uten slik informasjon er det fare for at mange vil overtre personregisterloven uten å være klar over det. Dette er uheldig.

2.5.3. Elektronisk betalingsformidling - problemer for Datatilsynet

For Datatilsynet vil elektronisk betalingsformidling og salgspunktterminaler innebære en sterkt økende arbeidsmengde, idet det vil bli opprettet mange nye personregistre med detaljerte personopplysninger.

Som det fremgår av fremstillingen i neste avsnitt, vil denne typen registere ikke være helt trivielle i personvernsammenheng. Sålenge opplysningene brukes etter sitt formål - til intern kontroll og avregning i butikk/betalingsinstitusjon - er de ikke særlig problematiske. Hvis de derimot tas ut av sammenheng og sammenstilles med andre opplysninger og brukes til andre formål, kan det lede galt avsted.

For Datatilsynet vil det med den nåværende loven være vanskelig å "sile" ut de viktige spørsmålene som knytter seg til slike systemer fra de mer trivielle spørsmålene, som kan være gjenstand for selvregulering.

2.5.4. Personvernproblemer - elektronisk betalingsformidling

2.5.4.1. Betalingsformidling og interessen i fullstendighet

I elektronisk betalingsformidling er det begrenset hva som registreres av opplysninger. Som nevnt ovenfor under avsnitt 2.5.1, kan det være opplysninger om navnet på kjøperen, kontonummeret til kjøperen, inngående balanse på kontoen, utgående balanse på kontoen, hva som er kjøpt, hvor det er kjøpt, og når det er kjøpt. I den betalingsinstitusjonen der vedkommendes konto er opprettet vil det selvfølgelig være registrert en rekke opplysninger i tillegg, alt avhengig av hvor omfattende kundeforhold vedkommende person har hos betalingsinstitusjonen.

Den informasjonen som registreres er svært knapp, og den vil nødvendigvis gi et ufullstendig bilde av den enkeltes bevegelser og forbruk. Systemene registrerer bare de tilfellene der det foretas handlinger som setter dem i aksjon - de registrerer ikke noe om årsaker, de registrerer ikke forbruk som betales kontant, de registrerer ikke om man bare handler for egen regning eller om man også handler på vegne av andre (foreldre, barn, naboer etc.). De registrerer ikke årsaker til at man tilfeldigvis befant seg i nærheten av akkurat den butikken på akkurat det tidspunktet.

Brukt til kontroll, revisjon og avregning internt i betalingsinstitusjonen, vil denne informasjonen etter alt å dømme være fullstendig og korrekt nok. Hvis man derimot benytter den til å forta vurderinger av berettigelsen av en persons tilstedeværelse i et bestemt område på et bestemt tidspunkt, eller slutninger om muligheter for et så høyt forbruk på en bestemt inntekt, vil opplysningene etter min oppfatning være meget ufullstendige. Det må derfor være viktig å sørge for at opplysningene bare blir brukt for sine rette formål. Siden opplysningene kan misbrukes, kan det etter min oppfatning også bli spørsmål om de i det hele tatt bør registreres. Opplysninger som først er registrert vil lettere kunne bli misbrukt på senere stadier.

2.5.4.2. Betalingsformidling og interessen i å være opplyst

Interessen i å være opplyst vil i utgangspunktet normalt være oppfylt i relasjon til ordinær bruk av opplysningene i betalingsformidlingen. Det er imidlertid på det rene at systemene vil bli mer kompliserte enn tidligere. Selv om den enkelte har gått frivillig inn på en ordning der de nevnte opplysningene blir registrert, vil det bli stadig vanskeligere å holde oversikt over hvordan opplysningene

blir brukt, hvordan de "flyter" rundt, og hvem som har tilgang til dem.

Bruk av elektroniske betalingsformidlingssystemer vil være basert på tillit mellom betalingsinstitusjonen og kunden. Det bør derfor være klart angitt overfor kunden hvem utenfor betalingsinstitusjonen som vil få adgang til opplysningene, og i hvilke tilfelle dette vil skje.

2.5.4.3. Betalingsformidling og interessen i diskresjon

Som jeg allerede har vært inne på, vil den enkelte stort sett være kjent med at de opplysningene som registreres vil bli brukt internt i henholdsvis bank og forretning til avregnings- og kontrollformål. Det blir imidlertid en viktig oppgave å sørge for at opplysningene bare brukes for slike formål.

Diskresjonsinteressen kommer etter min oppfatning inn i tre forskjellige relasjoner. For det første vil den enkelte betalingsinstitusjon sitte inne med mer detaljert kunnskap om sine kunder. Denne informasjonen er samlet inn for å kunne kontrollere og verifisere at bestemte transaksjoner har funnet sted. Kunden vil imidlertid også ha andre relasjoner til sin bank enn bare å bruke den som betalingsformidler. Skal banken f.eks. få anledning til å bruke en analyse av slike transaksjonsopplysninger som grunnlag for vurdering av en lånesøknad? Det blir etter min oppfatning viktig å trekke grensen for hva det skal være tillatt å bruke opplysningene til. Dette er et spørsmål om kundens "rettssikkerhet" i forholdet til betalingsinstitusjonen.

Dernest er det et spørsmål om hva personer som betjener bankterminaler, men som ikke er ansatt av banken (f.eks. kassapersonale i et supermarked), skal få adgang til av opplysninger om den enkelte kunde som vil ha utført banktjenester. Dette forutsetter at det opprettes bankterminaler i supermarked, der den enkelte kunde kan få utført visse banktjenester. Bankenes eget personale har taushetsplikt, de gjennomgår en viss opplæring der det bl. a. legges betydelig vekt på diskresjon mv. Vil supermarkedsterminalene (som kan brukes til flere banktjenester enn bare å belaste kontoen for dagens handel, bl. a. til kontantuttak og innskudd, saldoutskrift, betalingsoverføring osv.) medføre at det skjer en uthuling av denne opparbeidede diskresjonsplikten fra bankenes side? Vil butikkinnehavere kunne bruke terminalene til å gjøre sine undersøkelser vedrørende kundene? Svaret på slike spørsmål vil selvfølgelig avhenge av hvordan systemene bygges opp, og hvem som autoriseres til å bruke dem. Her vil jeg bare peke på at det eksisterer diskresjonsproblemer som det er viktig å ta stilling til før systemene bygges opp.

For det tredje vil mer detaljert forbruksinformasjon kunne brukes for kontroll- og etterforskningsformål av forskjellige myndigheter. Dette kommer jeg nærmer tilbake til nedenfor under avsnitt 2.5.4.5.

2.5.4.4. Betalingsformidling og interessen i borgervennlig administrasjon

I denne sammenheng er det nærliggende å bruke "borgervennlig administrasjon" synonymt med "publikumsvennlig", eller "forbrukervennlig" eller "kundevennlig".

Elektronisk betalingsformidling vil såvidt jeg kan bedømme ta over mer og mer av betalingsformidlingen i samfunnet. Utviklingen vil nok ikke gå så raskt som mange av teknikkens forkjempere har spådd - og det kan skje endringer i utviklingens retning. Systemene tas i bruk først og fremst fordi de skal være kostnadsbesparende - både for betalingsformidlingsinstitusjonen og for betalingsmottakeren.

Hvorvidt systemene vil innebære et overveiende antall fordeler eller et overveiende antall ulemper for publikum, vil også for denne typen systemer avhenge av hvordan de tas i bruk. Det er imidlertid helt nødvendig å gi lettfattelig, oversiktlig og fullstendig informasjon om hva som registreres i systemene, hva de kan brukes til, hvordan de fungerer, hva som er forskjellen til nåværende betalingssystemer mv. Det er dessuten viktig at systemene blir laget slik at det er enkelt for kundene til en hver tid å holde seg orientert om saldo, kredittgrenser, gebyrbestemmelser, rentebelastninger, krav om overføringer mellom forskjellige kundekonti ved overtrekk osv.

Det må dessuten legges vekt på å utforme reservesystemer, som gjør det mulig å få gjøre transaksjoner selv om elektronikken er satt ut av funksjon for kortere eller lengre perioder.

Det er etter min oppfatning en klar fare for at innføring av elektronisk betalingsformidling i stort omfang for alminnelige forbrukere, i første omgang vil føre til visse vanskeligheter med oversikten over og styringen av egen økonomi - i ethvertfall for relativt store grupper med alminnelige forbrukere.

2.5.4.5. Elektronisk betalingsformidling og interessen i å unngå overdreven kontroll

Som nevnt ovenfor under avsnitt 2.5.1, innebærer de nye salgspunktterminalene og de nye betalingsformidlingssystemene at det blir laget en mengde "elektroniske spor" som kan brukes til analyser og antakelser om hva folk har foretatt seg.

Markedsforskningsinstitusjoner vil kunne være interessert i opplysningene for å undersøke folks forbruksvaner, eller for å utforske mer raffinerte metoder for påvirkning av forbrukerne. Den ytterste konsekvens av slik bruk, vil kunne innebære ren manipulering av forbrukere via slik sammenkopling av forskjellige typer systemer, som er beskrevet ved et eksempel fra USA ovenfor under avsnitt 2.5.1.

Videre vil opplysninger fra slike systemer høyst sannsynlig finne veien inn i kredittopplysningsbyråenes registere over "dårlige betalere". Et sentralt spørsmål her, blir i hvilken grad transaksjonsopplysninger hos en betalingsformidlingsinstitusjon skal kunne danne grunnlag for betalingsanmerkninger og kredittvurderinger hos et kredittopplysningsforetak. Det er satt grenser for det i den någjeldende lovgivningen, men det er spørsmål om de er dekkende.

Betalingsformidlingsopplysningene vil også skape problemer i forhold til myndighetene ønske om å drive kontroll og etterforskning. Skattemyndighetene kan være interessert i å bruke analyser av forbruksmønsteret til å vurdere om forbruket står i rimelig forhold til inntekten. Sosial- og trygdemyndighetene kan være interessert i det samme, for å vurdere tilståelse av behovsprøvede stønader etc. Politiet vil kunne være interessert i å bruke slik informasjon i etterforskningsøyemed - i første omgang når det foreligger mistanke mot en bestemt person, for å finne ut om vedkommende har kjøpt inn mistenkelige varer, har overført penger til andre mistenkte personer, har hatt unormalt høyt forbruk, har oppholdt seg på mistenkelige steder osv. - i neste omgang kan slik informasjon tenkes benyttet preventivt, for analyser av forbruksvaner hos personer som er i "faresonen", og som kan komme til å gjøre noe kriminelt.

Det vil være vanskelig å gardere seg mot en lovbestemt utvidelse av myndighetenes kontrolladgang og adgang til å benytte slike registre for kontroll- og etterforskningsøyemed. Dette er noe som bør tas med i betraktning når systemene planlegges. Det kan være at systemene bør lages slik at transaksjonsopplysninger registreres i minst mulig omfang. Dersom opplysningene først er registrert, vil det være svært vanskelig å gardere seg mot at de blir tatt i bruk - først i konkrete saker der det er mistanke om noe kriminelt - dernest for mer generelle kontrollformål, ut ifra den tanken at den lovlydige ikke har noe å skjule.

2.6. On-line diagnose og feilretting av EDB-utrustning

2.6.1. Utrustning - muligheter

Mange maskinleverandører tilbyr etter hvert "on-line" programservice. Dette innebærer at de f.eks. fra sitt

service-senter i utlandet gis direkte adgang - via telefonlinje - til maskinens hukommelse, for å kunne analysere og rette opp feil. Denne formen for programservice er noe forskjellig fra leverandør til leverandør, men hovedprinsippet er det samme.

Leverandørene krever ofte en fri adgang til å gjøre dette på tidspunkter som passer dem selv, for fritt å kunne legge opp sine egne arbeidsrutiner. Under slik feilretting, vil de kunne ha behov for å kunne foreta en utskrift av sentrallageret i maskinen, for å kunne analysere innholdet av denne. En slik utskrift (fullstendig utskrift i maskinkode, gjerne representert i det oktale eller det heksadesimale tallsystem), vil kunne inneholde alle, eller deler av de data som for øyeblikket befinner seg i sentrallageret.

Fordelene med en slik ordning ut fra effektivitetsmessige betraktninger er åpenbare. Feilfinning og oppretting av feil kan i stor utstrekning utføres fra diagnosesenteret, uten at kostbart personell behøver å reise over store avstander.

2.6.2. On-line diagnose - problemer for registereierne

I en del tilfelle vil on-line diagnosesystemer innebære en overføring av personopplysninger til utlandet. Formålet med en slik overføring vil ikke nødvendigvis være at det i utlandet skal opprettes et personregister, men dette vil kunne bli konsekvensen av en overføring. For de som har installert et EDB-anlegg, og som benytter seg av on-line feildiagnose, vil den någjeldende ordningen i personregisterloven innebære at de må melde fra til Datatilsynet om at slik feildiagnostisering finner sted. Datatilsynet bør i tilknytning til slike ordninger kunne stille vilkår, som innebærer at datamaskinutrustningsleverandører skal ha begrenset adgang til å hente ut fortrolige personopplysninger fra sine kunders anlegg.

Dette påfører registereierne visse arbeidsbyrder når det gjelder å sende inn melding til Datatilsynet, og de vilkårene som gis fra Datatilsynets side vil medføre at det legges opp arbeidsrutiner og sikringskrav som kan være tyngende.

On-line feildiagnose vil kunne være en belastning for registereierne også i et annet henseende. Dersom det blir alminnelig kjent at registereiere med personregistre som inneholder sensitive opplysninger benytter seg av on-line feildiagnose, og det blir kjent at personopplysninger mer eller mindre kontrollert kan hentes ut av en utenlandsk leverandør, vil dette være egnet til å gi et meget uheldig bilde av vedkommende registereier. Registereiere som er avhengig av et godt tillitsforhold til sine kunder bør i egeninteresse, og for å beskytte opplysninger om registrerte personer, være meget restriktive med å la leverandører få uhindret adgang til registrerte opplysninger.

2.6.3. On-line diagnose - problemer for Datatilsynet

Det någjeldende system etter personregisterloven er at det skal sendes en melding til Datatilsynet ved overføring av konsesjonspliktige personregistre til utlandet, eller ved overføring av personopplysning til utlandet, når hensikten er å føre personopplysningen inn i et register i utlandet, som ville vært konsesjonspliktig dersom dette ble ført i Norge.

Det foreligger svært få meldinger om overføring av personopplysninger eller personregistre til utlandet. Mye tyder på at personregisterlovens bestemmelser på dette punkt ikke overholdes. Datatilsynet har betydelige problemer med å holde oversikt over hvilken flyt av data som foregår ut av landet. On-line diagnosesystemer reiser ikke problemer for Datatilsynet som er spesielle sett i forhold til en hvilken som helst annen overføring til utlandet.

Mange som benytter seg av on-line diagnosesystemer, er ikke er klar over at dette kan innebære en overføring av personopplysninger til utlandet, som skulle vært meldt fra til Datatilsynet, slik at Datatilsynet eventuelt kunne nedlegge et forbud mot overføringen. Dette er et problem for Datatilsynet.

Etter hvert som slike feilfinnings- og diagnosesystemer blir mer utbredt, vil det dessuten kunne bli et betydelig sikkerhetsproblem.

2.6.4. Personvernproblemer - on-line diagnose

2.6.4.1. On-line diagnose og interessen i fullstendighet

Spørsmålet om fullstendighet har i og for seg ingen betydning sett i forhold til det som er formålet med on-line diagnosesystemer. Hensikten med en slik overføring vil aldri være å benytte opplysningene som overføres til noen form for beslutning eller informasjonsvirksomhet som har betydning for den opplysningene beskriver. Etter sitt formål, skal en slik overføring bare tjene til en analyse som tar sikte på å rette opp feil i maskin eller programutrustning hos den som fører vedkommende register.

2.6.4.2. On-line diagnose og interessen i å være opplyst

Interessen i å være opplyst vil sjelden være oppfylt i forhold til on-line diagnosesystemer. Interessen i å være opplyst vil i hovedsak rette seg mot det registeret som eventuelt blir gjenstand for overføring. Et sentralt spørsmål blir om den enkelte også skal informeres om at slike opplysninger eventuelt kan komme til å bli overført til en maskinleverandør i utlandet, dersom det i

fremtiden skulle bli nødvendig med en overføring for diagnoseformål. Det vil være vanskelig å få oppfylt interessen i å være opplyst i forhold til slike systemer.

2.6.4.3. On-line diagnose og interessen i borgervennlig administrasjon

Dersom on-line diagnose virker etter sin hensikt, skal den føre til at vedlikehold og feilretting på registereierens EDB-anlegg kan utføres raskere og rimeligere enn ved tradisjonelle former for vedlikehold. Forutsetningsvis vil dette føre til en mer "borgervennlig administrasjon". Feil på EDB-anlegg både i offentlig og privat administrasjon, kan som kjent føre til unødig irritasjon og forsinkelser i de tjenester borgerne mottar fra denne administrasjonen. Jo raskere feil kan lokaliseres og rettes opp, jo bedre vil service overfor publikum også kunne være.

Dessuten bør slik feilfinning og oppretting av feil kunne føre til reduserte vedlikeholdsomkostninger. I siste instans bør dette kunne føre til rimeligere service overfor det publikum som er registrert i registrene.

2.6.4.4. On-line diagnose - interessen i å unngå overdreven kontroll

Dersom opplysninger innhentet fra leverandørfirma for diagnoseformål, kun benyttes til feilfinning og oppretting av feil, vil opplysningene ikke kunne medføre noen økt kontroll.

I kontrollsammenheng er det imidlertid et aspekt som bør overveies nærmere. Selve det faktum at personopplysninger får en større spredning (blir overført til leverandør evt. i utlandet), innebærer en økt risiko for at opplysningene kan komme på avveie og bli misbrukt. Generelt vil vissheten om at slik mer eller mindre tilfeldig overføring av opplysninger til utlandet kan skje, også føre til en mer eller mindre begrunnet frykt for at opplysningene kan bli misbrukt til kontrollformål. Selv om jeg anser den reelle faren for kontroll via slik on-line diagnose for å være relativt liten, er det viktig å påpeke at slik overføring innebærer en uthuling av taushetsbestemmelser og regler som skal sikre opplysninger så lenge de befinner seg hos vedkommende registerfører.

2.7. Teledata - Tekst-TV

Den elektroniske teknologiens utvikling innebærer at forutsetningene for spredning og forbruk av informasjon vil kunne forandres radikalt. To nye informasjonsbærende medier, som er beregnet på å bli spredt til det store publikum, er tekst-TV og teledata.

Tekst-TV innebærer at tekst og enkle grafiske bilder via

vanlig TV-sendinger overføres til mottakerens TV-apparat. TV-apparatet må være utstyrt med en spesiell enhet. Tekst-TV kringkastes på samme måte som vanlige TV-sendinger. Det benyttes bare en annen frekvens enn for den ordinære TV-sendingen. Man antar i dag at tekst-TV kan brukes fornuftig blant annet til teksting av ordinære TV-program (f.eks. teksting for hørselssvekkede, eller teksting på ett eller flere fremmedspråk), eller for formidling av informasjon i form av annonser, nyheter, forbrukerundersøkelser e.l. Tekst-TV kan bare formidle en begrenset mengde informasjon. Det eksprimenteres i dag over hele den vestlige verden med forskjellige anvendelser av denne teknologien.

Teledata er bygget opp på en litt annen måte. Teledata innebærer at informasjon lagret i en eller flere datamaskiner, via telefonnettet overføres til en terminal, som f.eks. kan være et modifisert TV-apparat. Teledata har svært stor kapasitet. Forbrukerne vil gjennom dette mediet kunne velge i et stort tilbud av informasjon. I tillegg gir dette mediet en mulighet for å kommunisere begge veier, dvs. at forbrukeren kan sende beskjeder tilbake til datamaskinen eller til andre brukere av teledata. Således kan det f.eks. bygges ut til et system for bestilling av varer, bestilling av reiser, elektronisk post, opinionsundersøkelser, osv. Teledata kan ved en omfattende utbygging få en svært allsidig anvendelse. Eksempler som nevnes på bruksområder, er nyhetsformidling, samfunns-informasjon, annonseinformasjon og forbrukeropplysninger, og formidling av elektronisk post.

Den grunnleggende forskjellen mellom tekst-TV og teledata, ligger i at tekst-TV innebærer en kringkasting av en avgrenset mengde informasjon, som mottakeren kan ta i mot på sitt apparat. Dette er en enveis overføring av informasjon. Teledata derimot kringkastes ikke på samme måte som tekst-TV. Teledata er først og fremst en telefonopplysningstjeneste i databaseform. Opplysningene lagres i en datamaskin, som er koblet til telefonnettet. Ved å ringe opp datamaskinen, kan man på sitt TV-apparat få fram de opplysninger som man ønsker fra datamaskinen. Jeg skal ikke her gå inn på noen nærmere beskrivelse av teknisk utrustning og bruksmuligheter for henholdsvis teledata og tekst-TV. I det følgende vil jeg konsentrere fremstillingen om teledata, idet det først og fremst er denne teknikken som kan innebære problemer i personvern-sammenheng. Dette har sammenheng med at teledata i motsetning til tekst-TV er en toveis kommunikasjonsform, som innebærer at det vil bli registrert og lagret opplysninger om den enkelte forbruker.

Ovenfor under avsnitt 2.3 har jeg redegjort nærmere for hvilke problemer registrering av tjenestebruk kan medføre i slike systemer. Bruksregistreringsproblemene vil derfor ikke bli berørt nærmere i dette avsnittet. Her vil jeg bare påpeke at dersom teledata i årene som kommer blir utviklet - og får en utbredelse som samsvarer med det som forventes på eksperthold - vil de bruksregistrerings-registrene som opprettes omfatte svært mange mennesker,

og relativt detaljert informasjon om hva slags tjenester disse menneskene benytter seg av. Den forventede store spredningen slike systemer vil få, kan i seg selv innebære betydelige problem.

Her vil jeg kort redegjøre for enkelte problem forbundet med bruk av teledata som toveis kommunikasjonsmiddel. Av særlig interesse i dette henseende er den enkeltes rett til beskyttelse av de meddelelser som sendes via det nye mediet.

De problemer som oppstår for dette mediet i så henseende er ikke særlig forskjellige fra de problemer som ovenfor er beskrevet under avsnitt 2.3 om elektronisk post i sin alminnelighet - bortsett fra at dette mediet er basert på å bli forbrukerorientert, hvilket vil medføre en skalaforandring av dimensjoner. Videreutviklet vil problemene dessuten kunne bli av lignende art som nevnt ovenfor under punkt 2.5 i forbindelse med betalingsformidling - salgspunktterminaler.

Når det gjelder problemer for de forskjellige interessegrupperingene (registereierne, Datatilsynet, de registrerte), henviser jeg forsåvidt til diskusjonene ovenfor under avsnitt 2.3 og 2.5.

Her vil jeg bare påpeke at antallet elektroniske spor som samfunnsborgerne setter etter seg i slike systemer vil øke betydelig. En sterk utvidelse av tjenestespekteret som tilbys via slike systemer, vil samtidig føre til opprettelse av store mengder av personregistre, med informasjon som den enkelte registrerte person har sterke interesser i å beskytte overfor uvedkommende.

Felles for de fleste anvendelser av teledata, er at de opplysninger som blir formidlet, blir lagret i en datamaskin i forbindelse med overføringen. En slik sammenkobling av kommunikasjonsteknikk og EDB, fører til informasjonsbehandling som den nåværende personregisterlovgivning antakelig ikke passer særlig godt for. Ikke desto mindre vil det gjennom slike systemer opprettes en mengde personregistre som etter den nåværende lovgivningen skal konsesjonsbehandles.

Siden dette er forbrukerorienterte systemer, må det forventes at antallet registre kommer til å bli meget stort. Dette vil i sin tur føre til betydelige problemer både for de registrerte og for Datatilsynet.

2.8. Systemer for søking i fri tekst

Det arbeides i Edb-bransjen intenst med å finne fram til enklere og rimeligere måter for registrering av data, enn det man klarer i dag.

En registreringsteknikk som er kommet relativt langt, er optisk lesing av maskin- eller håndskrevne tekster.

Da trykkingen av Norges lover (lovsamlingen) ble lagt om til EDB fra 1981-utgaven, var en vesentlig del av registreringen gjort ved at den forrige utgaven ble lest optisk, side for side. Riktignok var kvaliteten ikke så god som den burde vært, hvilket ga et omfattende arbeid med korrekturlesing etter registreringen, men eksemplet viser at dette er en registreringsform som er fullt mulig. Teknikken er under stadig utvikling også på dette området, og det er grunn til å tro at fremtidig utstyr vil kunne lese relativt raskt og feilfritt.

En annen registreringsmåte som er kommet relativt langt, er registrering ved hjelp av Elektronisk tekstbehandling. Dette er nærmere behandlet ovenfor under avsnitt 2.2.

Etterhvert som enkle og rimelige dataregistreringsteknikker utvikler seg, blir et stadig mer viktig spørsmål å finne metoder for gjenfinning (søking) av bestemte opplysninger i det som er registrert. Både det som registreres ved optisk lesing av maskinskrift/håndskrift, og det som registreres ved ETB, vil ofte være ustrukturert informasjon, sett ut fra EDB-synspunkt. Det finnes imidlertid i dag EDB-systemer som er spesielt utformet med sikte på gjenfinning av informasjon i store samlinger av fri tekst. Vi kaller gjerne slike systemer for "fritekst-søkesystemer" (NOVA*STATUS, SIFT, STAIRS, IMDOC osv.).

Forskjellen mellom ETB-systemene og fritekst søkesystemene sett fra personvernsynspunkt, er vel nærmest at fritekst søkesystemene er mye mer effektive til å finne fram den ønskede informasjon fra store dokumentmasser.

Jeg vil understreke at ETB sett i sammenheng med fritekst søkesystemer, skaper muligheter som etter min oppfatning er bekymringsfulle sett fra personvernsynspunkt. Hvis man tar vare på det som skrives i ETB-systemene, og gjør det søkbart i fritekstsystemene, blir det bl.a. mye lettere å finne fram til informasjon om bestemte personer som finnes i den registrerte teksten. Som kjent arbeides det med innføring av slikt samspill mellom ETB og fritekstsøkesystemer i domstolene. Dersom dette innføres på landsbasis, blir det mulig å søke etter bestemte navn for å finne ut om bestemte personer har vært involvert i bestemte typer rettssaker - som part, som vitne, som sakkyndig, som dommer etc. (medmindre det innføres en regel om at domsutskrifter skal anonymiseres før de gjøres søkbare i fritekstsystemer). Det er grunn til å påpeke at dette gir muligheter for bruk av domsutskriftene på helt andre måter enn tidligere.

Vi kan tenke oss en rekke andre områder hvor tilsvarende teknikk kan tas i bruk. Dersom f. eks aviser tar slik teknikk i bruk for å gjøre avisartikler søkbare (hvilket allerede er gjort i USA), vil dette dramatisk forandre betydningen av det som skrives i avisene. Personer som omtales må bli mye mer påpasselige med til enhver tid å ta opp og dementere/kreve beriktigelse av det som eventuelt er feil. I dag har avisene den fordel sett ut

ifra interessen i diskresjon, at det meste som skrives der, glemmes relativt fort. Dersom kombinasjonen ETB/fritekstsøking tas i bruk, vil derimot det som står i avisartikler som er registrert, svært raskt kunne finnes tilbake, for å bli brukt i bestemte sammenhenger.

De fleste av de større avisene har tatt i bruk ETB. Med alle vår tids forskjellige politiske opprop og underskriftskampanjer, politisk debatt, oppslag av kriminalsaker og skandaler, vil slike systemer etter min oppfatning være en alvorlig trussel mot interessen i diskresjon. Dette gjelder særlig hvis slike systemer gjøres kommersielt tilgjengelig f.eks for arbeidsgivere som skal foreta ansettelser, låneinstitusjoner som skal yte lån osv.

2.9. Oppsummering - teknologisk utvikling

Den tekniske utviklingen vil slå igjennom også på en rekke andre områder enn de som er nevnt i den oversikten jeg har gitt foran. Problemene disse teknikkene vil reise, er på mange måter parallelle til de som er nevnt ovenfor. I tillegg finnes en del teknikker som medfører problemer utover de som er tatt opp ovenfor. Dette er særlig forskjellige former for overvåkningsteknologi, som vil bli benyttet av forskjellige myndigheter i fremtiden. Som eksempler kan nevnes "det intelligente kort" som kan benyttes som identifikasjonskort. Dersom slikt kort tas i bruk som tvungent identifikasjonskort, har det tekniske muligheter som etter min oppfatning gjør det særdelses problematisk, ut i fra personverninteressene.

Videoovervåkningssystemer, stemmegjenkjenningssystemer, fingeravtrykkssystemer og andre såkalte "pattern recognition"-systemer reiser særlige problemer, som fortjener grundige overveielser ut fra personvernsynspunkter. Slike systemer er såvidt spesielle, at plassen her ikke tillater nærmere behandling.

Jeg har her bare gitt en relativt kortfattet og summarisk påpeking av enkelte områder som skaper spesielle problemer, og der den teknologiske utviklingen fører til at det vil skje en rask utvikling av nye typer registre. Det er særdeles viktig for Datatilsynet å følge med på slike nye områder, for ikke å bli hengende etter den tekniske utviklingen og bli et "sandpåstrøingsorgan" for løsninger fastlagt av andre. Datatilsynet har i dag ikke ressurser til å kunne utføre systematisk arbeid med sikte på å holde seg a jour med den tekniske utviklingen. Dette er etter min oppfatning meget bekymringsfullt.

3. MULIGE ENDRINGER I REGELVERKET

3.1. Innledning - oversikt

I utredningsoppdraget pkt. a), ble jeg bedt om å

"utrede mulige endringer i regelverk (lov og forskrifter), og administrative rutiner som kan foretas for å begrense Datatilsynets arbeidsbyrde uten at det i vesentlig grad antas å ville ha uheldige virkninger for personvernet."

Det kan konstateres at Datatilsynets arbeidsbyrde ved gjennomføringen av det någjeldende regelverket, er for stor i forhold til bemanningen. Dette er f. eks. kommet klart til uttrykk i Datatilsynets årsmelding for 1981 (St. meld. nr. 103 1981-82. Se bl. a. avsnitt 2.1.1, og 2.2, samt kapittel 5).

Datatilsynet har i dag en arbeidsordning internt som er gjennomrasjonalisert. Saksbehandlerne er utstyrt med EDB-terminaler, og konsesjoner skrives direkte av dem, ved hjelp av standardiserte konsesjonsvilkår som er lagret i tekstbehandlingssystemet. Behandlingen av mange konsesjoner for registre som føres likeartet i lokale og regionale forvaltningsorganer, er standardisert - og utstedes på grunnlag av koordinerte søknader som sendes Datatilsynet fra sentralt hold.

Arkivet i Datatilsynet er EDB-basert, og saksbehandlerne kan finne fram tidligere avgjorte saker meget raskt ved hjelp av sine terminaler. Dette er en meget god hjelp i forbindelse med de mange telefonhenvendelser Datatilsynet får, og i forbindelse med den løpende saksbehandlingen. Ingen saker behandles i mer enn to trinn, og forelegg av saker for Datatilsynets styre holdes så lavt som mulig - bare viktige prinsippspørsmål blir behandlet der. Datamaskinbasert arkivføring letter arbeidet på Datatilsynets forværelse betydelig. Med en såvidt liten stab som Datatilsynet har i dag, vil derfor ytterligere forenklinger i de administrative ikke kunne medføre nevneverdige begrensninger i Datatilsynets arbeidsbyrder.

Regelverket er i dag såvidt komplisert i sin utforming, at det er meget vanskelig for publikum å orientere seg i det. Kompleksiteten skyldes at loven er utformet med en mengde fullmaktsbestemmelser, og at det i henhold til disse er gitt forskrifter på flere nivåer (kgl. res. og beslutninger av Justisdepartementet). Ytterligere forsøk på å begrense Datatilsynets arbeidsbyrder ved å gi forskrifter i henhold til den någjeldende loven, ville føre til en økende kompleksitet. Dette ville etter min oppfatning være svært uheldig. Jeg vil derfor i det følgende konsentrere fremstillingen om grunnleggende endringer i selve personregisterloven. Bare gjennom slike endringer vil Datatilsynets arbeid kunne forenkles

vesentlig.

I det følgende vil det først bli redegjort for hvordan personverninteressene ivaretas gjennom den någjeldende personregisterloven (avsnitt 3.2). Dernest vil det bli gitt en oversikt over legalitetsprinsippets krav til presisjonsnivået i straffesanksjonerte materielle regler (avsnitt 3.3), og for personregisterlovens system og bakgrunn (avsnitt 3.4). Videre vil enkelte krav til innholdet eller til endringer i innholdet av personregisterloven bli gjennomgått (avsnitt 3.5). I avsnitt 3.6 foretas det en drøfting av mulige alternative måter å ivareta personverninteressene på, i avsnitt 3.7 og 3.8 gis visse anbefalinger om hvilket alternativ som er å foretrekke, og i kapittel 4 foreslås visse endringer i lovteksten som er nødvendige på bakgrunn av anbefalingene.

3.2. Hvordan er personverninteressene ivaretatt gjennom bestemmelsene i personregisterloven?

De fem "personverninteressene" som er oppstilt av Blekeli og Selmer (jfr. ovenfor under avsnitt 1.3.1), finner vi igjen i personregisterloven`s " kapittel 3 ("alminnelige regler"), og i kapittel 4 ("plikt til å søke samtykke til å opprette personregister"), samt i de regler som er fastsatt for det enkelte register - enten gjennom forskrifter for visse "typeregistre", eller ved konsesjonsvilkår for det enkelte register.

§ 6 gir anvisning på at bare relevante (eller nødvendige) opplysninger skal registreres. Dette kan ses som et direkte utttrykk for interessen i diskresjon: Den som bruker et register skal bare kunne få relevante opplysninger ut av det, når registeret benyttes for å finne fram informasjon som benyttes i en konkret beslutning. Opplysninger som ikke er relevante, (som det ikke er "tillatt" å ta i betraktning når beslutningen treffes), skal ikke finnes i registeret. Med andre ord: De skal holdes "hemmelig" for beslutningtakeren. Samtidig innebærer § 6 en stadfestelse av det generelle prinsippet om fair saksbehandling: Irrelevante opplysninger skal ikke inngå som grunnlag for en beslutning rettet mot den enkelte. Det er også denne bestemmelsen som er grunnleggende når et bestemt "typeregisters" innhold har blitt fastlagt ved forskrifter, eller når et enkeltregisters innhold blir fastlagt gjennom en konsesjon fra Datatilsynet.

§ 8 i personregisterloven er en stadfestelse av prinsippet om at registrerte opplysninger skal være fullstendige og korrekte, når de først ansees for å være relevante. Samtidig inneholder § 8 også bestemmelser om retting, sletting/supplering av registre, som ivaretar elementer av interessen i diskresjon. Videre står det i § 11 enkelte bestemmelser som innebærer at det i den enkelte konsesjon bør overveies regler som ivaretar denne interessen (jfr. f. eks. § 11 annet ledd pkt. 1), 2), 8), 9) og 10). Tilsvarende bestemmelser i noe mer

konkretisert form er tatt inn i forskriftene § 2-1, med virkning for de forskriftsregulerte registrene, og i konsesjonsvilkårene for de registrene som fortsatt konsesjonsbehandles.

Som nevnt foran er den enkeltes interesse i å være opplyst om hva som foregår, nærmest å anse som en forutsetning for oppfylling av de to forannevnte interessene. Denne interessen er ivaretatt i loven § 7, som gir den enkelte en rett til å få vite hva som er registrert om seg selv i det enkelte register (med visse begrensninger). I forskriftene kapittel 1 er det gitt nærmere regler om visse sider ved gjennomføringen av innsynsretten - først og fremst svarfrister ved henvendelser om innsyn etc., men også en viktig utvidelse av bestemmelsen i loven § 7 til også å gjelde for manuelle lønnstakerregistre i privat næringsvirksomhet, foreninger og stiftelser. I konsesjonsvilkårene kan Datatilsynet også fastsette unntak fra innsynsretten, og nærmere vilkår for den enkeltes bruk av innsynsretten. Rammene for innsynsretten er imidlertid gitt uttømmende ved § 7 i loven. Disse kan ikke utvides, hverken ved forskrift eller ved den enkelte konsesjon, ut over det § 7 selv gir direkte anvisning på.

Interessen i en borgervennlig administrasjon har ikke fått sitt uttrykk i materielle bestemmelser i selve loven (når man ser bort fra at § 7 om innsynsrett også er et viktig element i denne interessen). Det gis imidlertid i § 11 (som angir hvilke typer regler som bør overveies gitt i de enkelte konsesjoner) endel ledetråder for at loven også skal kunne brukes til å fremme denne interessen.

I § 11 annet ledd heter det således at det skal fastsettes slike vilkår for det enkelte register, som "kan begrense de ulemper opprettelsen og bruken av registeret ellers kunne medføre." Videre fremgår det i § 11 at det under konsesjonsbehandlingen særlig skal overveies fastsatt bl.a. regler om "omfanget og innholdet av den informasjon som skal gis ved meldinger eller andre henvendelser til den registrerte." Av forarbeidene til loven fremgår at man her har tatt sikte på å forebygge uforståelige, kodede EDB-utskrifter på forskjellige skjemaer, lønnsslipper, utbetalingsblanketter mv., som skrives ut ved hjelp av EDB. Særlig er det understreket at utskriftene i tillegg til selve resultatet av foretatte beregninger mv., bør inneholde opplysninger om grunnlaget for resultatet (jfr. NOU 1975:10, avsnitt 5.7.3).

Også bestemmelsen i § 11 annet ledd pkt. 1) vil bidra til å fremme en "borgervennlig administrasjon". Bestemmelsen innebærer adgang til å fastsette nærmere regler i den enkelte konsesjon om innsamling og kontroll av de opplysninger som tas inn i det enkelte register. Slike regler kan vel først og fremst sees som en ivaretakelse av interessen i at opplysninger skal være fullstendige og korrekte, men de har selvfølgelig også en vesentlig betydning for hvordan administrasjonen fremtrer overfor

publikum.

Interessen i å unngå overdreven kontroll, er på liknende måte ivaretatt gjennom bestemmelser i loven som gir anvisning på hva som skal overveies fastsatt av regler i den individuelle konsesjon. Særlig § 11 annet ledd - nr. 3) (om kobling av registre), nr. 4) (om personnummer), nr. 5) (om utlevering eller overføring av opplysninger fra et register til andre registre), nr. 10) (om sletting eller ikke-bruk av opplysninger etter en viss tid), og nr. 11) (om sikkerhetstiltak og tilintetgjøring av registre) - tar sikte på å ivareta interessen i å unngå overdreven kontroll.

I forskriftene § 2-1, er det gitt nærmere regler om de fleste av disse forholdene, med virkning for de registre som omfattes av forskriftene.

3.3. Legalitetsprinsippets krav til straffesanksjonerte materielle regler

I forrige avsnitt er visse trekk ved bestemmelsene i personregisterloven gjennomgått. Disse bestemmelsene gjelder i utgangspunktet for alle personregistre som omfattes av loven. De gir generelle anvisninger på vurderinger som må gjøres av Datatilsynet etter et relativt fritt skjønn (med unntak av innsynsretten, som er relativt klart avgrenset).

Ved utforming av vage, skjønnsmessige regler som sanksjoneres ved straffebestemmelser, vil man lett komme i konflikt med legalitetsprinsippet, slik dette er angitt i grunnloven § 96. Det fremgår der at ingen kan straffes uten etter lov. Dette innebærer at det ikke er adgang til å utforme straffebestemmelser der det straffbare forhold er helt upresist angitt i loven. Bratholm (Anders Bratholm, "Strafferett og samfunn", Universitetsforlaget 1980) formulerer dette slik (s. 85):

> "Kravet om lovhjemmel innebærer også at det straffbare forhold ikke kan være helt upresist angitt i loven. Det ville f.eks. være i strid med legalitetsprinsippet å gi et straffebud som generelt retter seg mot handlinger som krenker andre eller som er i strid med offentlige interesser. Dette ville være til så liten veiledning for borgerne, eller for retten som skulle anvende "loven", at det ville være jevngodt med ingenting. Men helt presise kan straffebud ikke være. De må nødvendigvis overlate en del til skjønnet, og i enkelte tilfelle ganske meget. F.eks. retter endel straffebud seg mot den som opptrer "urimelig" eller "utuktig" på et nærmere bestemt område. Se f.eks. prisl. § 18 som setter forbud mot urimelige priser m.v. og strl. § 211,1. ledd bokstav b, som rammer bl.a. utbredelsen av utuktige skrifter. Slike straffebud som overlater meget til dommerskjønnet, kalles gjerne for rettslige standarder. Det er større betenkeligheter ved å godta dem på strafferettens område enn utenfor, men heller ikke i strafferetten

kan de altså helt unngås."

Legalitetsprinsippet innebærer som det fremgår av dette, at det må stilles opp relativt faste kriteria for at noe skal være straffbart. Dette medfører at dersom bestemmelsene i personregisterloven skal være straffesanksjonerte, må de gi klare anvisninger på hva det straffbare består i. Bestemmelsen i § 6 i loven lar seg således ikke direkte straffesanksjonere.

Den enkelte registerfører må ikke stilles overfor muligheten for å bli straffet fordi han selv har en annen forståelse av hva som er relevante opplysninger enn det f. eks Datatilsynet har.

Når det imidlertid foreligger en autoritativ fortolkning fra Datatilsynet gjennom et vedtak etter § 8, annet ledd, eller gjennom et konsesjonsvedtak etter § 10, er det ikke lenger noe problem å straffesanksjonere den manglende oppfølgingen av dette vedtaket. Vedtaket vil gi den nødvendige anvisning på hva som er relevant registrering.

3.4. Personregisterloven`s system - bakgrunn

Foran i avsnitt 3.2 antydes hva som er personregisterloven`s system: Enkelte, tildels skjønnsmessige, materielle bestemmelser i loven, samt et vidtgående konsesjonssystem med vide fullmakter for Datatilsynet til etter fritt skjønn å vurdere hva som er relevante opplysninger, og til å gi regler om bruk, oppbevaring, behandling, sletting sikring osv. av opplysningene.

Et viktig poeng med dette systemet, er at straffebestemmelsene i loven bare gjelder overfor overtredelser av regler som har et relativt klart angitt materielt innhold. Det heter om dette i Odelstingsproposisjon nr. 2 1977 - 78, s. 61, spalte 1:

> "Etter departementets forslag til straffebestemmelse for enkeltpersoner i § 38 vil ikke enhver overtredelse av lovens materielle regler være straffbar. Det er gjort unntak for enkelte bestemmelser som etter sitt innhold er så ubestemte og skjønnsmessige at straff verken vil være rimelig eller hensiktsmessig."

Det fremgår av det som er sagt ovenfor at dette skyldes legalitetsprinsippets krav om angivelse av hva som er straffbart.

Bakgrunnen for at dette system ble valgt da loven ble vedtatt, var vanskeligheter med å formulere bestemmelser som tilstrekkelig klart kan angi grensene for lovlig personregistrering. Seip-utvalget drøfter dette spørsmålet (NOU 1975:10) på s 51-52. Utvalget konkluderer som følger:

> "Etter utvalgets mening er det i en sak som dette vanskelig å finne en tilfredsstillende løsning

utelukkende basert på forholdsnormer. Det er vanskelig å peke på løsninger som kan gjennomføres uten unntak eller modifikasjoner: Hvis man forsøker å gi en regel for forvaltningen generelt, må den bli meget fleksibel. Den tyske proposisjonen viser dette.

Dersom man tildeler et sentralt forvaltningsorgan kompetanse til å avgjøre hva som skal være tillatt eller ikke tillatt, avhjelpes disse mangler. Man kan få presise regler for det enkelte system, og fordi et slikt opplegg tillater en individuell vurdering, kan man gå lengre i retning av å legge vekt på sikkerhetssynspunkter m.m., enn om samtlige system skulle behandles under ett. Dessuten vil et slikt opplegg lette den politiske kontroll. De organer som avgjør spørsmålet om samtykke, får et overordnet ansvar for utviklingen. Den tyske proposisjonen lar de forskjellige forvaltningsorganer hver for seg ha eneansvar.

På denne bakgrunn mener utvalget at en konsesjonsordning må spille en vesentlig rolle også i en norsk datalov. Dette betyr ikke at man bør se bort fra muligheten av å gi forholdsnormer. Det er grunn til å gi enkelte bestemmelser som fastsetter en ramme som konsesjonsmyndigheten bør handle innenfor eller som angir en normalløsning."

Odelstingsproposisjon nr. 2 1977 - 78 inneholder en omfattende gjengivelse av synspunkter fra Seip-utvalgets utredning, og fra høringsuttalelsene, som tildels var omfattende på dette punktet. Etter denne gjengivelsen konkluderes det på følgende måte (Odelstingsproposisjon nr. 2 1977 - 78, s. 32, sp. 1):

"Etter Justisdepartementets syn er de aktuelle alternativene enten en konsesjonsordning eller en ordning med meldeplikt kombinert med adgang for Kongen til å fastsette regler ved forskrift eller for det enkelte register. - Motargumentet mot å innføre en konsesjonsordning for offentlige personregistre er frykten for at det må bygges opp et relativt stort apparat til å behandle konsesjonssøknadene. Det vil koste penger, og det er mulig at det i en tid framover vil samle seg opp restanser. Med en meldepliktordning ville Datatilsynet muligens kunne konsentrere seg mest om de registrene som det mente reiste de største problemene fra et personvernsynspunkt. - Det kan også nevnes at overfor registre som brukes i statlig virksomhet, har storting og regjering allerede i dag i prinsippet gode midler til å påvirke utviklingen - ved instruksjonsmyndigheten og bevilgningsmyndigheten.

Justisdepartementet mener likevel at man bør innføre en konsesjonsordning. Dette gir den største sikkerheten for at hvert enkelt register blir vurdert ut fra personvernhensyn. Blant annet på grunn av den usikkerhet mange mennesker synes å føle overfor moderne personregistre, er det viktig i størst mulig grad å holde utviklingen under kontroll. Dertil kommer

at det etter Justisdepartementets mening gjerne vil hefte diverse svakheter ved meldepliktsordninger som kontrollsystem, bl.a. at kontrollen gjerne kommer inn i etterhånd. Videre er det vel også slik at skal en meldeplikt fungere som en reell kontroll, krever dette også et nokså omfattende arbeid fra kontrollorganets side. En er derfor ikke overbevist om at den arbeidsmessige forskjell mellom konsesjonsplikt og meldeplikt er så stor som det ofte hevdes."

Som kjent ble Justisdepartementets forslag bifalt i Stortinget. Av Odelstingsproposisjon nr. 2 1977 - 78 fremgår at Justisdepartementet ikke anså en ordning med forholdsnormer for å være noe aktuelt alternativ: Valget sto etter departementets oppfatning mellom konsesjon eller meldeplikt. Det skinner igjennom i departementets argumentasjon at det anser et system basert på forholdsnormer, som skal gjelde generelt for alle typer personregistre, for å måtte bli såvidt generelt utformet, at det vil være vanskelig å understøtte med straffesanksjoner.

Dette synet har etter min oppfatning fremdeles gyldighet. Jeg vil imidlertid nedenfor under avsnitt 3.6 - 3.8 komme nærmere tilbake til mulige alternativer til en konsesjons- eller meldepliktordning i kombinasjon med skjønnsmessige forholdsnormer.

3.5. Krav på endringene utenfra

3.5.1. Synspunkter i Stortinget

Under Stortingets behandling av Datatilsynets årsmelding for 1980, besluttet Stortinget den 25.mars 1981 å oversende til Regjeringen følgende forslag fremsatt av representanten Carl I. Hagen:

"Det henstilles til Regjeringen å vurdere:

1. Opphevelse av konsesjonsplikten for personregistre og satsing på vanlige lover og regler med selvkontroll, men med straffeansvar.

2. Frigjøring av Datatilsynet fra Justisdepartementet.

3. Innføring av strenge regler for sammenkopling av registre, og like plikter for offentlige som for private registre.

4. Tilintetgjørelse av innholdsfortegnelsen over personregistre."

I forbindelse med Stortingets behandling av Justisdepartementets budsjett for 1982, den 23.november 1981, ba stortingsrepresentant Hanna Kvanmo Justisministeren vurdere om det kunne finnes en annen

instans i forvaltningen som mer uavhengig kunne føre kontroll med Datatilsynet. Dette tilsvarer pkt. 2 i forslaget ovenfor.

Da personregisterloven ble vedtatt, innstilte flertallet i Justiskomiteen på at Datatilsynets styre skulle oppnevnes av Stortinget, etter forslag fra Regjeringen. Det var imidlertid enighet i komiteen om at Datatilsynet skulle være et frittstående organ underordnet Kongen. (Innst. O. nr. 47 - 1977-78, s. 5).

I brev av 11.5.82, fra Justisdepartementet til meg, påpekes det at endel av de nevnte spørsmål har sterk tilknytning til utredningsprosjektet, og det anmodes om at jeg så langt det er mulig skal kommentere spørsmålene.

3.5.2. Europarådets konvensjon - OECD's guidelines

Det er utformet internasjonale regelverk til ivaretakelse av personverninteresser, først og fremst innenfor to internasjonale organisasjoner som Norge er medlem av: OECD og Europarådet.

Innenfor OECD er det laget et sett med retningslinjer, som ikke formelt sett er bindende, men som i praksis oppfattes slik, for de av medlemslandene som har gitt sin tilslutning til dem. Norge har gitt sin tilslutning. Retningslinjene er gjengitt i vedlegg 5. Generelt kan det sies at vår nåværende lov tilfredsstiller kravene i retningslinjene. Videre vil kravene som stilles av Europarådskonvensjonen (se nedenfor) hovedsaklig dekke det samme som retningslinjene.

Europaroparådets konvensjon om persondatabeskyttelse er undertegnet av Norge, men den er ennå ikke ratifisert. Den trer ikke i kraft før den er ratifisert av minst 5 stater. Det er ventet at Norge vil ratifisere i relativt nær fremtid, og at konvensjonen tidligst vil være bindende i løpet av 1983.

I konvensjonen er fastlagt endel grunnleggende prinsipper for persondatabeskyttelse. Kapittel 2, artikkel 4, pkt. 1, pålegger det enkelte land å ta de nødvendige forholdsregler i intern lovgivning for å ivareta de grunnleggende prinsipper om persondatabeskyttelse, slik de er angitt i konvensjonens kapittel 2. Konvensjonen i engelsk tekst er gjengitt i vedlegg 4.

Konvensjonens krav er rammebetingelser for hvilke endringer som kan foreslås. En endret personregisterlov må oppfylle konvensjonens grunnleggende prinsipper.

3.6. Alternative reguleringsmåter

3.6.1. Innledning

Jeg tar for gitt at vi fortsatt skal ha et organ som skal følge med og være vaktbikkje for personverninteressene. Dette har vi forsåvidt forpliktet oss til gjennom Europarådskonvensjonen (jfr. vedlegg 4, artikkel 13), og det synes å være bred enighet om det.

Et hovedspørsmål som bør diskuteres nærmere, er hva slags organ dette skal være. Da personregisterloven ble vedtatt, ville de borgelige partiene at Datatilsynets styre skulle utnevnes av Stortinget, men at Datatilsynet forøvrig skulle være et forvaltningsorgan under Justisdepartementet. Det ble imidlertid den gangen bestemt at Datatilsynet skulle være et forvaltningsorgan, underlagt regjeringen. Størstedelen av den utøvende myndighet etter loven, er lagt til regjeringen.

Spørsmålet om hvorvidt Datatilsynet skal sortere direkte under Stortinget, eller om det skal sortere under regjeringen, har avgjørende betydning for hva slags myndighet Datatilsynet skal ha.

Underlagt Stortinget antar jeg at Datatilsynet må være et rent ombudsmannsorgan - med rett til å ta opp bestemte saker, kreve opplysninger, avgi uttalelser mv. - men uten myndighet til å nedlegge forbud mot bestemt virksomhet, eller til å treffe avgjørelse i saker av forvaltningsmessig karakter. Jeg har ikke funnet konkrete holdepunkter for at det må være slik, men det er vel nærliggende å støtte seg til det alminnelige maktfordelingsprinsippet.

Underlagt regjeringen, står man i prinsippet fritt til å tillegge Datatilsynet myndighet. Datatilsynet blir da en del av forvaltningen på samme måte som i dag.

Det er imidlertid ikke noe iveien for at Datatilsynet kan gis en mer selvstendig og uavhengig stilling selv om det er en del av forvaltningen. Eckhoff (Torstein Eckhoff: Forvaltningsrett, Tanum-Norli, Oslo 1980), sier følgende om dette (s.201):

> "Stortinget kan (ved lov eller plenarvedtak) bestemme at et organ helt eller delvis skal være unndratt fra Regjeringens (og andre forvaltningsorganers) instruksjons- og organisasjonsmyndighet. Unntak gjelder bare hvor de "kongelige prerogativer" kommer inn i bildet."

Eckhoff påpeker (s.204) at av uavhengige statsorganer, har vi først og fremst domstolene - men at det imidlertid også finnes endel andre organer som er gitt en mer eller mindre uavhengig stilling. Videre heter det hos Eckhoff om dette:

> "Ofte henger dette sammen med at de har fått oppgaver som stiller særlige krav til deres upartiskhet, f.eks. til å løse individuelle rettsspørsmål eller å avgjøre andre individuelle tvistespørsmål. Noen av dem har en

organisasjonsform og saksbehandling som ligner meget på domstolenes. I særlig grad gjelder dette Trygderetten som avgjør klager over trygdemyndighetenes avgjørelser, jfr. l 16/12 1966 nr. 9. Det er tydelig forutsatt i loven og dens forarbeider at hverken Regjeringen eller departementet skal ha noen instruksjonsmyndighet over Trygderetten - bortsett fra den myndighet loven (jfr. §§ 4 og 33) gir Regjeringen til å gi utfyllende regler om "arbeidsordning og administrasjon" mv. - - - Også organer som i noe mindre grad enn Trygderetten har domstollignende arbeidsoppgaver og saksbehandling, er gitt ganske stor selvstendighet.

Som eksempel kan nevnes Prisrådet som har til hovedoppgave å avgjøre forskjellige typer av tvister mellom næringsdrivende og klager over visse avgjørelser av Prisdirektoratet (jfr. l. 26/6 1953 nr. 4 §§ 4, 23, 33 siste ledd, 34 siste ledd, 37, 40 og 41). Rådet må rette seg etter de generelle retningslinjer for prispolitikken som fastsettes av Regjeringen (§ 3). og eventuelt av Stortinget (§ 14), men forøvrig kan det neppe anses undergitt noen instruksjonsmyndighet. Dets avgjørelser kan omgjøres av departementet (§ 49), men dette skjer praktisk talt nesten aldri.

Andre eksempler er de klagenemnder som er opprettet i medhold av forskjellige lover (jfr. f.eks. bankinspeksjonsloven av 7/12 1956 nr. 1 § 6 og loven om merverdiavgift av 19/6 1969 nr. 66 § 57), kontrollkommisjonene i det psykiske helsevern (l. 28/4 1961 nr. 2 kap III) og Styret for det industrielle rettsvern (l. 2/7 1910 nr. 7, jfr.l. 3/3 1961 nr. 4 § 12 og nr. 5 § 3, l. 15/12 1967 nr.9 § 8 og l. 29/5 1970 nr.33 § 9). Ingen av disse kan instrueres om hva de enkelte avgjørelser skal gå ut på. Derimot kan det gis generelle instrukser om saksbehandlingen og i noen av tilfellene også om realitetsspørsmål.

Heller ikke Riksskattestyret kan instrueres om hva det individuelle vedtak i klagesaker skal gå ut på (jfr. l. 18/8 1911 nr. 8 § 105 flg.). Hvorvidt det også inntar en uavhengig stilling når det gir generelle uttalelser om ligningsspørsmål, har det vært delte meninger om, jfr. Ingvaldsen-utvalgets innstilling (NOU 1972:38) s. 20-21 og s. 25-26. Etter utvalgets oppfatning taler de beste grunner for at Riksskattestyret må rette seg etter departementets og Regjeringens oppfatning når det gjelder fortolkning av skatteloven."

Av Ingvaldsen-utvalgets innstilling (NOU 1972:38), s. 20-21, fremgår det at i tilfelle hvor det er klare holdepunkter i lov eller i forarbeider, er det ikke noe prinsipielt i veien for at et forvaltningsorgan gjøres uavhengig av regjeringen. Utvalget konkluderer imidlertid med at etter en helhetsvurdering må forvaltningen hovedsaklig bygges opp slik at Regjeringen og departementene har instruksjons- og kontrollmyndighet

overfor andre organer. Det tar imidlertid en reservasjon med hensyn til visse typer organer. Således heter det bl.a. på s. 24, sp. 1:

> "Utvalget har heller ikke noe å bemerke til at det legges til uavhengige organer å ta avgjørelse i saker hvor sterke rettssikkerhetsgrunner taler for en slik løsning, En kontroll fra departementets side vil også ha som formål å sikre gode, rettferdige avgjørelser, men det kan virke naturlig i en del saker at en kontroll ut fra rettssikkerhetshensyn legges til organer som ikke står under politisk overledelse, sml. foran om kontrollkommisjonene etter lov om psykisk helsevern og Trygderetten." (Uthevet her, AF)

Utenriks- og konstitusjonskomiteen i Stortinget sluttet seg til utvalgets utredning på dette punktet, jfr. Innst. S. Nr. 277 - 1976-77, s. 8-9. Komiteen konkluderer slik på dette punktet:

> "Komiteen ser det i det hele som maktpåliggende at man etter hvert kommer frem til ordninger hvor fravær av regjeringens og departementenes instruksjons- og kontrollmulighet blir unntakstilfelle som er spesielt begrunnet."

Denne hovedregel bør etter komiteens oppfatning bare fravikes i spesielle tilfelle, bl.a. der hvor sterke rettssikkerhetshensyn tilsier at vedkommende organ arbeider selvstendig.

Etter personregisterloven slik den er i dag, er den utøvende myndigheten etter loven i det alt vesentlige lagt til regjeringen. Det meste av den myndighet som er tillagt Datatilsynet, er delegert fra regjeringen ved forskrift gitt ved kgl. res., eller ved forskrift gitt ved beslutning av Justisdepartementet. Dette innebærer at regjeringen (og departementet etter fullmakt fra regjeringen) har en vidtgående kompetanse til å instruere Datatilsynet.

Såvidt jeg kan forstå skyldes endel av den kritikken som har vært reist mot organiseringsmåten slik denne er i dag, at Datatilsynet formelt sett i for stor grad er en del av det alminnelige forvaltningsapparat - et forvaltningsapparat som samtidig er innehaver av de langt fleste av de samlingene med personopplysninger som virkelig reiser personvernproblemer. Dette er ikke egnet til å gi inntrykk av at Datatilsynet er et organ som er istand til å ivareta personverninteresser overfor det samme forvaltningsapparatet. Etter min oppfatning taler derfor sterke rettssikkerhetsgrunner for at Datatilsynet skal gjøres mer uavhengig av forvaltningen.

I denne sammenheng vil jeg påpeke at dette er et spørsmål som tillegges stor betydning av tilsynsorganene i hele den vestlige verden. På sitt årlige møte for samarbeid og utveksling av erfaringer, som i år ble holdt i London i oktober, vedtok representantene for tilsynsorganene en uttalelse med følgende ordlyd:

"The conference recognises the need in all countries for a mechanism independent of government and other authorities that has power to investiate non-complinace with an individuals legal right

- to know subject to protection of the general public interest and the privacy rights of third parties, what records are maintained about the individual concerned

- to know the purpose for which personal information is collected

- to ensure that such records are relevant, accurate, complete and up-to-date and to make annotations if corrections are not made or accepted by the collector or storer of the records

- to know the uses (including transfer to other countries) made of such records and to be protected from uses not connected to the purpose for which the data was originally collected."

Dersom man f.eks. direkte i loven legger myndigheten på endel punkter til Datatilsynets administrasjon, og oppretter Datatilsynets styre som klageinnstans, (jfr. Skattedirektorat - Riksskattestyre), vil Datatilsynet kunne gjøres mer uavhengig av den øvrige utøvende del av forvaltningen.

Regjeringen vil fortsatt kunne utøve en viss kontroll med Datatilsynet - ved oppnevning av styret for Datatilsynet, og ved den budsjettmessige kontroll med Datatilsynets virksomhet.

Innenfor det sistnevnte alternativet er det mulig å gi Datatilsynet en varierende grad av myndighet i forhold til innsamling, lagring og bruk av personopplysninger. Ytterpunktene vil under dette alternativet representeres ved en ren ombudsmannsliknende virksomhet på den ene siden, og et forvaltningsorgan med en sterk myndighet til å treffe vedtak av forvaltningsmessig karakter (konsesjoner - forbud) på den andre siden.

3.6.2. Materielle bestemmelser om innsamling lagring og bruk av personopplysninger - uten organ

I forbindelse med diskusjonene av hvordan personvernspørsmålene bør reguleres, har det stadig fra flere hold vært hevdet at personregisterloven bør inneholde materielle bestemmelser om hvordan det skal være tillatt å samle inn, lagre og bruke personopplysninger - kombinert med straffebestemmelser for eventuelle overtredelser.

Allerede i någjeldende personregisterlov er det endel materielle bestemmelser. Dette gjelder både bestemmelsene i kapittel 3 i loven (relevansprinsippet i § 6, innsynsretten i § 7 og rettingsplikten i § 8), og en

rekke av bestemmelsene i virksomhetskapitlene i loven.

Ytterligere skritt i denne retning vil kunne gjøres på flere måter.

I sin mest rendyrkede form ville dette innebære en fullstendig opphevelse av konsesjonsplikten og nedleggelse av Datatilsynet. Det ville i såfall bli opp til den enkelte å forfølge sin rett via de vanlige kanaler - f. eks ved klage til overordnet forvaltningsorgan over forvaltningsavgjørelser, eller ved domstolene i den utstrekning prosesslovgivningens krav til rettslig interesse mv. er tilfredsstillet.

Som nevnt allerede innledningsvis, anser jeg ikke dette for å være noe aktuelt alternativ. Dette ville dessuten stride mot artikkel 13 i Europarådets konvensjon om persondatabeskyttelse (se vedlegg 4), som Norge vil ratifisere i nær fremtid.

3.6.3. Materielle bestemmelser - ombudsmann

Neste trinn er materielle regler kombinert med et organ med rene ombudsmannsfunksjoner - men uten kompetanse til å treffe vedtak som inneholder påbud eller forbud. I kombinasjon med et slikt organ, kan man tenke seg forskjellige grader av foreleggsplikt i saker som berøres av personverninteresser (men med en kompetanse for organet kun til å avgi uttalelser).

I den svakeste varianten, ville organet bare kunne ta opp saker av eget tiltak, eller på grunnlag av henvendelser utenfra.

I den sterkeste varianten vil organet kunne ta opp saker av eget tiltak og etter henvendelse utenfra, i tillegg til at det kan etableres en vidtgående plikt til å innhente en uttalelse fra organet i saker som berører personverninteresser (lovutkast, forskriftsutkast og enkeltvedtak om opprettelse og utforming av samlinger av personopplysninger, datasikkerhet, dispensasjon fra regler om taushetsplikt, kobling av opplysninger, utlevering av opplysninger i maskinlesbar form osv).

Mellom disse ytterpunktene er det rom for forskjellige grader av foreleggsplikt for et slikt organ. Jeg ser ikke grunn til å gå nærmere inn på dette i denne omgang.

Et organ av denne typen kan både legges under Regjeringen, og under Stortinget.

3.6.4. Materielle regler - organ med beslutningsmyndighet

En organisering av en noe annen karakter får vi, dersom man både har materielle regler, og et organ som har beslutningsmyndighet i forhold til innsamling, lagring og bruk av personopplysninger.

Som nevnt foran vil et organ med selvstendig beslutningsmyndighet sannsynligvis måtte legges til forvaltningen.

Også under en ordning med et organ som har selvstendig beslutningsmyndighet, kan man velge alternative former for regulering. En nærliggende måte å skille mellom de forskjellige alternativene på, vil følge av hvilke hjemler som er gitt for inngrep overfor de som samler inn, lagrer og bruker personopplysninger.

For det første kan man ha en ordning der organet har kontrolladgang, og adgang til å ta opp saker av eget initiativ, men hvor det ikke foreligger noen plikt til å forelegge konkrete saker for organet. Dette er ordningen for de ikke konsesjonspliktige registrene (manuelle personregistre uten "sensitive opplysninger"), og de forskriftsregulerte registrene i dag (personregisterloven § 6 jfr. § 8, og § 9 jfr. § 5).

Et neste skritt i retning av kontroll, er en ordning der det fastlegges visse rammer i loven for hva som skal være tillatt, samtidig som det åpnes for en dispensasjonsadgang, der Datatilsynet etter en konkret vurdering kan gi tillatelse til at bestemte opplysninger brukes på andre måter enn loven foreskriver.

Dernest kan man ha en meldepliktsordning (notifikasjon). En slik ordning innebærer at organet skal ha en melding om opprettelse av bestemte samlinger, eller om bestemte former for bruk, men innebærer i og for seg ikke at det kreves en formell tillatelse. Dersom kontrollorganet skal ha en fortegnelse over bestemte grupper av slike samlinger av personopplysninger, for å bidra til informasjon mv. overfor publikum, er det nødvendig å ha en form for slik notifikasjon.

Meldepliktsordningen kan kombineres med kontrolladgang og adgang til å nedlegge forbud mot - eller adgang til å stille vilkår for - bestemt innsamling, lagring eller bruk av personopplysninger. Meldepliktsordning kan dessuten gjøres gjeldende bare for visse innsamlings- lagrings- eller bruksformål, eller for bruk av bestemte typer tekniske hjelpemidler, eller for bestemte typer opplysninger. Som allerede nevnt, vil en eller annen form for meldeplikt være en klar forutsetning for å opprette og opprettholde en eller annen form for fortegnelse over samlinger, slik som loven § 4 i dag foreskriver.

Endelig kan man ha den ordningen vi har i dag - En konsesjonsplikt, der det kreves tillatelse for å få lov til å samle inn, lagre eller bruke personopplysninger for bestemte formål, for å føre opplysninger med bestemte hjelpemidler, eller for å lagre bestemte typer opplysninger. Dette alternativet kan kombineres med en

meldepliktsordning som nevnt ovenfor, og med kontrolladgang og adgang til å nedlegge forbud eller stille vilkår som nevnt ovenfor. Dagens ordning er en variant av dette alternativet, som selvfølgelig kan utformes på flere måter.

Alle de foran nevnte alternativene kan kombineres med noe helt nytt, som man nå vil innføre i Sverige: En lisensplikt for de som vil føre personopplysninger på EDB (Denne kan eventuelt kombineres med en plikt for lisensinnehavere til å sende inn en fortegnelse over typer av opplysninger f.eks. en gang pr. år. Dette lot man være i Sverige).

Denne ordningen innfører man der, til erstatning for en meget vidtgående konsesjonsplikt for personregistre på EDB. Ordningen innebærer at alle som vil føre personregister på EDB må ha en lisens fra Datainspektionen, og de skal være ført opp i Datainspektionens fortegnelse over licensinnehavere. I tillegg er det innført noen flere materielle regler enn tidligere, samtidig som konsesjonsplikt er foreslått opprettholdt for registre ut fra visse kriterier (innhold, formål).

Den ordning man nå innfører i Sverige fører til omtrent det samme omfang av konsesjonsplikt for EDB-registre der, som vi har i Norge i dag - mens vi her i tillegg har konsesjonsplikt for manuelle registre.

3.7. Valg av alternativ

3.7.1. Hva er best ut ifra personverninteressene?

Som nevnt foran i avsnitt 3.2, er personregisterloven`s system i dag at det er gitt enkelte, tildels vage og skjønnsmessige, materielle bestemmelser i loven, samt et vidtgående konsesjonssystem med vide fullmakter for Datatilsynet (egtl.: Regjeringen) til etter fritt skjønn å vurdere hva som er relevante opplysninger, og til å gi regler om bruk, behandling, sletting, sikring osv. av opplysningene.

Etter min oppfatning er det fremdeles grunn til å tro at et konsesjonssystem vil gi den beste garanti for at hver enkelt samling av personopplysninger blir vurdert ut ifra personvernhensyn (jfr. Justisdepartementets begrunnelse for valg av konsesjonsalternativet gjengitt ovenfor under avsnitt 3.4). Ut fra de erfaringer Datatilsynet har, er det mye som tyder på at selve informasjonsverdien av konsesjonsvilkår som den enkelte registeransvarlige får tilsendt i posten, og som retter seg direkte til den enkelte registeransvarlige, er betydelig bedre enn av tilsvarende regler gitt i forskrifts, eller i lovs form.

En meget viktig side ved konsesjonssystemet, er dessuten at det enkelte registeropplegg forutsettes prøvet på

forhånd, før det foretas omfattende investeringer i utforming av systemer, og i anskaffelse av utstyr. Det har ofte vært poengtert at Datatilsynets vurderinger bør foretas såvidt tidlig i utredningen av nye systemer, at det får en reell innflytelse på den endelige utformingen av systemene. Datatilsynet har en rekke ganger avgitt forhåndsuttalelser om anvendelse av bestemte personregistre. Slike forhåndsuttalelser vil selvfølgelig kunne innhentes også under et system med vage forholdsnormer, som kan presiseres gjennom konkrete forbud (med virkning framover), fastsatt av Datatilsynet. Jeg frykter imidlertid at sålenge det ikke foreligger noen plikt til å forelegge saker for Datatilsynet på forhånd, så vil det sjelden bli noen slike forespørsler.

Dette vil kunne komme til å medføre et alvorlig problem sett ut fra personvernhensynene, fordi det vil være ennå vanskeligere å argumentere for de relativt vage personverninteressene når det allerede er foretatt omfattende investeringer i bestemte løsninger.

Min konklusjon er derfor at det beste alternativ for regulering av bruk av personopplysninger fortsatt er det system vi har i loven i dag: Enkelte, relativt vage forholdsnormer - kombinert med konsesjonsplikt eller eventuelt forskriftsregulering av individuelle registre/registertyper.

Som påpekt ovenfor, vil forholdsnormer gitt i lovs form måtte være så vage og generelle at det ikke vil være mulig i praksis å knytte sanksjoner til overtredelse av dem. Jeg vil imidlertid nedenfor komme nærmere tilbake til en mulig metode for regulering ved relativt vage forholdsnormer - kombinert med adgang for Datatilsynet til å nedlegge forbud mot bestemt virksomhet.

3.7.2. Behov for personalressurser under ulike alternativ

Ovenfor under avsnitt 3.6, har jeg gått gjennom forskjellige måter for ivaretakelse av personverninteressene. Den viktigste forskjellen på de alternativene som er gjennomgått, refererer seg til hva slags oppgaver og kompetanse et eventuelt organ med ansvar for personvern skal ha. Jeg har tatt som forutsetning at den materielle regulering av adgangen til å samle inn, lagre eller bruke personopplysninger, stort sett skal ha det samme innhold under de forskjellige alternativene. Eller sagt på en annen måte: De forskjellige personverninteressene skal ivaretas på tilsvarende måte under alle alternativene.

I dette avsnittet vil jeg fremsette enkelte overslag over behovet for personalressurser under de forskjellige alternativene. Jeg vil knytte overslagene til hovedalternativene, uten å gå i detalj om forskjellige varianter innenfor de enkelte av disse.

Materielle regler - uten organ

Det første alternativet, innebærer en nedleggelse av Datatilsynet, samt en utforming av mer detaljerte materielle regler enn vi har i dag, for å ivareta personverninteressene. Dette ville innebære en innsparing av hele Datatilsynets årlige budsjett, men det ville antakelig føre til en viss merbelastning på det ordinære domstolsapparatet. Graden av merbelastning ville antakelig avhenge av hvor grundig kjennskap det alminnelige publikum ville få til sine rettigheter etter de materielle reglene. Som nevnt ovenfor under avsnitt 3.6.2, anser jeg dette ikke for å være et aktuelt alternativ, idet personverninteressene etter min oppfatning ville bli for dårlig og tilfeldig ivaretatt.

Ombud

Det neste alternativet som er nevnt, innebærer at vi får et sett materielle regler som skal ivareta personverninteressene, samtidig som vi får en ombudsmann som katalysator for, og vern om disse interessene. En ombudsmann ville måtte ivareta alle de oppgaver Datatilsynet har i dag - bortsett fra konsesjonsbehandlingen. Dette innebærer at det må finnes ressurser til å avgi prinsippielle uttalelser om utredninger, stortingsmeldinger, lov- og forskriftsforslag mv. som omhandler bruk av personopplysninger, og til å foreta selvstendige utredninger, til å avgi uttalelser i enkeltsaker som involverer personvernspørsmål, til å svare på henvendelser fra publikum og foreta undersøkelser etter anmodning fra publikum. Dessuten må det drives en aktiv informasjonsvirksomhet, og de ansatte i Datatilsynet må drive en meget aktiv egenutvikling ved deltakelse på konferanser og kurs mv. for å holde seg a jour med den tekniske utviklingen og utviklingen i bruk av den tekniske utrustningen.

Hvis vi ser på enkelte av de øvrige ombud som er opprettet i de senere år, vil vi se at disse tildels har en betydelig større bemanning enn Datatilsynet: Forbrukerombudet, som ble opprettet i 1973, er i Statskalenderen for 1982 oppført med 19 ansatte i konsulentstillinger eller høyere. I tillegg kommer 1.sekretærer og kontorpersonale. Likestillingsombudet (opprettet omtrent samtidig som Datatilsynet) er samme sted oppsatt med 7 i konsulent- eller høyere stilling. Også her kommer 1.sekretærer (saksbehandlere) og kontorpersonale i tillegg.

Dersom Datatilsynets arbeidsoppgaver som ombud skulle kunne utføres tilfredsstillende og med rimelig kontinuitet, vil jeg anta at Datatilsynet måtte ha en bemanning på omlag 12 personer (fire mer enn i dag). Disse kunne fordeles med 4 på forværelsetjenester, 6 utredere/saksbehandlere, 1 kontorsjef og 1 ombudsmann. Av utrederne/saksbehandlerne måtte minst 1 ha høyere utdannelse i EDB.

Det er imidlertid grunn til å påpeke at et ombud i ennå høyere grad enn et organ som gir tillatelser m.v., er avhengig av å nyte allmen tillit for å nå fram med sine synspunkter. Rekruttering av dyktige medarbeidere ville derfor bli særdeles viktig med en ombudsmannsordning. Bl.a. ville dette generelt kreve et noe høyere lønnsnivå for enkelte av stillingene i Datatilsynet.

Organ med beslutningsmyndighet

Det tredje alternativet jeg har nevnt, innebærer at man har et organ med beslutningsmyndighet i forhold til innsamling, lagring og bruk av personopplysninger, kombinert med materielle regler om det samme. En slik ordning kan utformes på mer eller mindre ressurskrevende måter.

Den minst ressurskrevende av disse, ville være et kontrollorgan med rett til å nedlegge forbud, men uten at det etableres noen plikt til å forelegge enkeltsaker for organet av eget tiltak. Et slikt organ ville såvidt jeg kan forstå måtte ha de samme funksjonene som en ombudsmann, og bemanningen måtte være omtrent tilsvarende: Det er i realiteten bare formen på beslutningen som vil være forskjellig. Ombudsmannen uttaler seg, mens et organ med beslutningsmyndighet enten kan uttale seg, eller nedlegge forbud. I det sistnevnte tilfellet vil vi riktignok få enkelte klagesaker, men de vil (ut fra erfaringene med den nåværende konsesjonsordningen) bli såvidt få, at det vil være lite merkbare forskjeller.

Noe mer ressurskrevende ville det være om man utformet mer detaljerte materielle regler enn hva vi har i dag, samtidig som Datatilsynet fikk tildelt kompetanse til å gi dispensasjoner fra disse reglene. (Dette er et alternativ der utgangspunktet er at bestemte former for føring av opplysninger er tillatt, mens alt annet er forbudt før det foreligger en uttrykkelig tillatelse - Den nåværende ordningen innebærer vel egentlig at alt er forbudt før uttrykkelig tillatelse foreligger.) Som jeg har vært inne på flere steder tidligere i denne utredningen, er det vanskelig å lage generelle materielle regler som i tilstrekkelig grad tilgodeser personverninteressene. Det må derfor antas at det under dette alternativet vil bli relativt mange dispensasjonssøknader - hvis man da ikke gjør de materielle reglene så utflytende at de bare i liten grad ivaretar personverninteressene. Jeg vil anta at dette alternativet derfor ville kreve en økning i antallet kvalifiserte saksbehandlere på tre i forhold til en ren ombudsmannsordning. I tillegg kreves det minst en person til i forværelsetjenester. Totalt ville en derfor komme opp i et bemanningsbehov under dette alternativet på rundt 16 personer.

En ordning som nevnt i forrige avsnitt kan bygges videre ut med en innføring av en meldeplikt for visse typer innsamling, lagring eller bruk av opplysninger mv. Dette medfører ikke behov for særlig økning i personalressurser

i forhold til forrige alternativ: Oppgavene vil være de samme, men det vil bli en viss økning i postmengden. Jeg antar derfor at det vil være behov for ytterligere en person i forværelsetjenestene under dette alternativ, slik at vi kommer opp i totalt 17 personer.

Den desidert mest ressurskrevende ordningen, er den som loven gir anvisning på i dag - En omfattende konsesjonsordning, både for manuelle registre og for registre ført ved EDB.

I tillegg til de funksjoner som utføres under de forannevnte alternativene, innebærer dette en relativt omfattende saksbehandlig for hver enkelt konsesjon. Dette vil imidlertid ikke uten videre være en arbeidsoppgave som kommer som tillegg til det som er nevnt foran: Den vil dels erstatte og overflødiggjøre enkelte av disse. Likefullt vil jeg anta at det ville være behov for en ytterligere styrking, slik at man totalt kommer opp i 20 ansatte. (Jeg forutsetter som sagt at man beholder nåværende ordning, samtidig som man sørger for tilstrekkelig informasjon, slik at både de som samler inn, lagrer og bruker personopplysninger, og publikum får kjennskap til personregisterlovens krav.)

3.7.3. Konklusjon

Ovenfor er forskjellige alternative måter for regulering av personverninteressene gjennomgått relativt overfladisk. Som nevnt avslutningsvis ovenfor i avsnitt 3.4, mener jeg at den nåværende ordning - med en relativt omfattende konsesjonsordning kombinert med forskrifter og enkelte materielle regler - fortsatt er den beste sett ut fra personverninteressene.

Denne ordningen sikrer dessuten at Datatilsynet har en løpende kontakt med databehandlingsmiljøet, slik at det kan foregå en kontinuerlig utveksling av synspunkter og erfaringer. Dette nære samspillet har etter min oppfatning vist seg å være svært verdifullt.

Jeg har imidlertid gjennom mitt utredningsoppdrag fått klare signaler som tilsier at det ikke hverken på kort eller lang sikt vil være aktuelt å øke bemanningen i Datatilsynet vesentlig. Det er derfor liten grunn til å utpensle de forskjellige alternativene særlig mye mer.

Siden vi på den ene siden forutsetter at det fortsatt skal være et Datatilsyn til å ivareta personverninteressene, og på den annen side forutsetter at det ikke er aktuelt på kort sikt å tilføre Datatilsynet økte ressurser av noen betydning, står vi tilbake med hovedspørsmålet om hvilken myndighet Datatilsynet skal ha, og hvilke arbeidsoppgaver det er realistisk å legge til Datatilsynet med dagens bemanning - slik at personverninteressene på slike premisser kan ivaretas best mulig.

Etter min oppfatning kan vi i utgangspunktet se bort fra

et alternativ der det opprettholdes noen form for konsesjonsplikt eller meldeplikt. Alle slike ordninger vil, etter det jeg kan forstå, kreve for mye rutinepreget arbeid for et organ av Datatilsynets størrelse, med den følge at viktig kontroll- og tilsynsarbeid blir skadelidende. Under den forutsetning at bemanningen i Datatilsynet ikke skal være særlig større enn den er i dag, er det ikke hensiktsmessig å benytte ressursene til å fortsette med en konsesjonsordning som forutsetter en bemanning på bortimot det tredobbelte. De knappe personalressursene som finnes i Datatilsynet må etter min oppfatning benyttes på utredninger av personvernspørsmål på prinsipielt grunnlag - i tilknytning til utviklingsprosjekter, offentlige utredninger, stortingsmeldinger, stortingsproposisjoner, odelstingsproposisjoner mv.

Også det nye svenske opplegget med lisens for de som fører visse opplysninger, vil etter min oppfatning innebære for mye rutinepreget arbeid for Datatilsynet. Dette ville dessuten innebære noe prinsipielt nytt, som krever relativt omfattende informasjonsopplegg og mye aktivitet fra Datatilsynets side for å bli gjort kjent. En stor fordel med dette systemet, er likevel at Datatilsynet langt på vei kunne gjøres selvfinansierende gjennom lisensavgiften. Det ville derved bli lettere å få gjennomført en oppbygning av Datatilsynet til et forsvarlig nivå.

Alternativet med et rent ombudsmannsorgan med uttalerett, underlagt Stortinget, ble i sin tid diskutert og forkastet i forbindelse med vedtakelse av personregisterloven. Argumentene mot et slikt organ, er vel først og fremst at man ikke kan gi et organ under Stortinget de nødvendige fullmakter til å treffe bindende vedtak om forvaltningens virksomhet. Videre har man fryktet at et slikt organ i for liten grad vil få direkte føling med databehandlingsbransjen, og derved ville stå for fjernt fra de praktiske problemene. Jeg antar at det på denne bakgrunn er hensiktsmessig allerede innledningsvis å sjalte ut også dette alternativet.

Etter dette står vi tilbake med et organ - administrativt underlagt forvaltningen - med ombudsmannsfunksjoner, og eventuelt med myndighet til å gripe inn overfor former for ulovlig registrering av opplysninger. Etter min oppfatning må et slikt organ ha vide fullmakter til å kreve opplysninger og til å gjøre kontroller hos de som samler inn, lagrer eller bruker opplysninger. Videre bør det etter min oppfatning være et organ med myndighet til å nedlegge forbud, og til å oppstille vilkår for å få lov til å fortsette med bestemt virksomhet. Et slikt organ må få tillagt eksklusiv beslutningskompetanse direkte i loven, for å sikre den nødvendige selvstendighet i forhold til forvaltningen.

Et særspørsmål oppstår i forhold til "registre" som er besluttet opprettet ved egen lov - hva enten disse føres i organ for stat og kommune eller i privat virksomhet - og i forhold til "registre" som er besluttet opprettet av

regjeringen. Dette er et spørsmål som reiser særlige problemer, som er dårlig løst i den någjeldende loven.

Det er vel noe tvilsomt om Datatilsynet kan gis en myndighet, som innebærer at det kan nedlegge forbud mot noe som er tillatt - eller endog pålagt - etter en bestemt lov. Det mest nærliggende i slike tilfelle må være at Datatilsynet skal sjaltes inn i selve lovgivningsprosessen som høringsinstans - og at Datatilsynet selvfølgelig fritt kan ta opp, og uttale seg om, det som allerede er lovregulert.

Ikke fullt så tvilsomt vil det være å gi Datatilsynet en adgang til å nedlegge forbud mot en bestemt virksomhet besluttet av regjeringen - eller et forvaltningsorgan underlagt denne.

Regjeringen vil alltid ha den utvei at den kan fremme et forslag til lovregulering av vedkommende virksomhet - hvilket vil heve den ut av Datatilsynets myndighetsområde i overensstemmelse med det som er sagt ovenfor.

3.8. Vurdering av den foreslåtte endringen

Som det fremgår ovenfor anser jeg den foreslåtte ordningen for å være den best mulige ut ifra den forutsetning at Datatilsynet i overskuelig fremtid ikke vil få vesentlige økninger i personalressurser.

Å opprettholde den nåværende ordningen uten å tilføre tilstrekkelige personalressurser, vil etter min oppfatning bety en dårlig ivaretakelse av personverninteressene. Datatilsynet er i dagens situasjon iferd med å bli oversett av databehandlingsmiljøet, fordi det sitter begravet i konsesjonssøknader, og fordi det er en skremmende mangel på kjennskap til personregisterloven og forskriftene. For å få en mer utadvent og aktiv profil, må de ressursene Datatilsynet har til rådighet benyttes mer til kontrollvirksomhet og utredningsvirksomhet innenfor bestemte sektorer. Dessuten må det satses betydelig på informasjonsvirksomhet - både overfor publikum om deres rettigheter - og overfor de som samler inn, lagrer og bruker personopplysninger om deres plikter.

Ved den foreslåtte ordning mister man den direkte kontakten mellom Datatilsynet og brukerne av personopplysninger, som kravet om utfylling og innsending av konsesjonssøknader - og mottakelse av individuelt utformede konsesjonsvilkår innebærer. Dette er etter min oppfatning en alvorlig ulempe. Vi har på de områder som i dag er forskriftsregulert i en rekke tilfelle observert at kjennskapen til forskriftenes innhold er relativt dårlig, mens det virker som om kjennskapen til individuelt utformede konsesjonsvilkår (riktignok på andre områder) jevnt over er bedre. Når brukerne av personopplysninger mottar individuelt utformede konsesjonsvilkår som de ikke forstår, henvender de seg ofte til Datatilsynet for å oppklare eventuelle

uklarheter mv. Dette virker positivt for forståelsen av personvernproblematikken.

Baksiden av dette forhold er dessuten at Datatilsynet mister den relativt gode løpende kontakten med hva som skjer av utvikling innenfor databehandling av personopplysninger, som konsesjonsbehandlingen gir. Den foreslåtte ordningen krever derfor at det blir mulig å etablere andre ordninger som kan innebære at Datatilsynet får en slik kontakt.

Til en viss grad kan vel denne kontakten opprettholdes ved at Datatilsynet driver en utadvent virksomhet gjennom kontroller innenfor utvalgte sektorer. Videre er det nødvendig for de ansatte i Datatilsynet å drive en aktiv egenutvikling ved deltakelse på kurs og seminarer mv. innen bransjen, både som foredragsholdere og som deltakere. Den løpende kontakten med de enkelte opplysningsbrukerne vil imidlertid falle bort.

4. TVILSSPØRSMÅL - ENDRINGER I LOVEN

4.1. Innledning

Den ordningen som er antydet ovenfor krever at det gjøres endel endringer i lovens sentrale bestemmelser om konsesjonsplikt mv. I utredningsoppdraget pkt. c), ble jeg bedt om å

"Gjennomgå Datatilsynets erfaringer hittil, med sikte på å kartlegge tvilsspørsmål som har oppstått, og som det er viktig å få avklaret for Datatilsynets virksomhet. Forslag til løsninger ønskes utarbeidet der det er mulig innen prosjektets ressursrammer."

I forrige kapittel er det redegjort for noen mulige endringer i selve hovedprinsippene for personregisterlovgivningen. Disse endringsforslagene vil i det følgende bli tatt med i forslaget til endrede lovbestemmelser.

Etter hver enkelt § vil det bli redegjort nærmere om hvilke tvilsspørsmål de har medført. Forandringer i §§ er streket under. Den fullstendige teksten i den någjeldende loven er gjengitt i vedlegg 1.

4.2. Endringer i kap. 1

§ 1

> Loven gjelder for <u>innsamling, lagring og bruk av personopplysninger, og for visse typer virksomhet.</u>
>
> <u>Med personopplysninger er ment opplysninger og vurderinger som direkte eller indirekte kan knyttes til identifiserbare enkeltpersoner, sammenslutninger eller stiftelser.</u>
>
> <u>Loven gjelder for bruk av personopplysninger i organ for stat eller kommune og i privat næringsvirksomhet, foreninger eller stiftelser.</u>
>
> <u>Kongen (Alternativ: Styret i Datatilsynet) kan bestemme at loven også skal gjelde for innsamling, oppbevaring og bruk av personopplysninger som foretas av andre.</u>
>
> Kongen (Alternativ: Styret i Datatilsynet)kan bestemme at loven ikke skal gjelde for visse typer innsamling, lagring og bruk av personopplysninger.

§ 1 er den bestemmelsen som avgrenser lovens område. Bestemmelsen slik den er gjengitt ovenfor, inneholder for

det første en legaldefinisjon av "personopplysning". Denne definisjonen finnes også i den någjeldende loven, og den ser ut til å være tilfredsstillende i praksis.

I den någjeldende loven, er i tillegg en legaldefinisjon av "personregister" sentralt for avgrensningen av lovens område. Denne definisjonen innebærer et krav om at personopplysninger skal være "lagret systematisk slik at opplysninger om den enkelte person kan finnes igjen". Dette skiller seg noe fra det tilsvarende begrepet i svensk og dansk lovgivning.

Begrepet slik det står i dag medfører enkelte praktiske problemer, som man vel kan ta stilling til gjennom en tolkning fra sak til sak - om problemet kommer på spissen. Det blir imidlertid stadig tydeligere at registerbegrepet i sin nåværende form er kunstig. Det er mer nærliggende å begrense enhver form for innsamling, lagring og bruk av personopplysninger, idet de moderne hjelpemidlene relativt lett vil kunne brukes til å finne opplysninger fram, uten at de på forhånd er "lagret systematisk."

Det vekker fra tid til annen noe forundring blant de det angår, at personregisterloven regulerer opplysninger om "juridiske personer". Når det nå er aktuelt å begrense omfanget av arbeidet for Datatilsynet, bør det vurderes om man skulle avgrense loven til bare å gjelde fysiske personer. Man vil i såfall stå tilbake med et problem i forbindelse med småselskaper mv. der det er vanskelig å skille mellom person og selskap. Ved en eventuell revisjon av loven bør dette spørsmålet overveies nærmere. Etter min oppfatning vil det imidlertid i mange tilfelle foreligge behov for beskyttelse av opplysninger om "juridiske personer", som langt på vei er paralelle med de som gjelder for opplysninger om fysiske personer. Selv om de hensynene som ligger bak behovet for beskyttelse vil være noe forskjellige for opplysninger om henholdsvis juridiske og fysiske personer, vil det derfor etter min oppfatning være hensiktsmessig å behandle dem felles. I mange samlinger av personopplysninger vil dessuten opplysninger om fysiske og juridiske personer være lagret om hverandre på en slik måte at det er umulig å skille. Forslaget her innebærer derfor ingen endring på dette punkt.

Loven i sin nåværende form omfatter ikke innsamling, lagring og bruk av personopplysninger som foretas av privatpersoner. I endel tilfelle har dette skapt problemer, f. eks. når hovedfagstudenter e.l. har foretatt innsamling av tildels meget sensitive opplysninger som skal brukes som grunnlag for skriving av hovedfagsoppgave e.l. Som regel har problemet latt seg løse ved at vedkommende forskningsinstitusjon som studenten har fått sin veiledning fra, har påtatt seg et ansvar for det "registret" som opprettes. I enkelte tilfelle har dette imidlertid ikke latt seg gjøre. Undersøkelsen har isåfall falt utenfor personregisterlovens område.

Stadig flere privatpersoner vil antakelig i tiden fremover skaffe seg mikrodatamaskiner for hjemme- og hobbybruk. Sålenge disse ikke brukes i "privat næringsvirksomhet, foreninger eller stiftelser", vil bruken ikke være underlagt begrensningene i personregisterloven.

Stort sett vil det vel være fornuftig å holde slik bruk utenfor. Utviklingen i bruk foregår imidlertid svært raskt. For å etablere en beredskap, bør loven derfor inneholde en hjemmel til å utvide loven til å gjelde også for innsamling, lagring og bruk av personopplysninger som foretas av privatpersoner.

Forskriftshjemmelen foreslås etter § 1, fjerde og femte ledd lagt til Kongen. Det bør imidlertid overveies nøye hvem som skal ha kompetanse til å gi forskrifter etter loven, idet den som har forskriftsmyndighet normalt også vil ha en instruksjonsmyndighet i relasjon til forskriften. Jeg har derfor satt opp Datatilsynets styre som alternativ forskriftsgivende myndighet.

4.3. Endringer i kap. 2

§ 2

> Det blir opprettet et Datatilsyn. Datatilsynet skal være et frittstående organ.
>
> Datatilsynet blir ledet av et styre, som skal ha 7 medlemmer. Medlemmene blir oppnevnt av Kongen, som også fastsetter hvem som skal være styrets formann og nestformann.
>
> (Alternativ:Datatilsynet blir ledet av en direktør, som tilsettes av Kongen)
>
> (Alternativ: Det opprettes et Styre for Datatilsynet. Styret skal ha 7 medlemmer. Medlemmene oppnevnes av Kongen, som også fastsetter hvem som skal være styrets formann og nestformann).
>
> Avgjørelser som treffes av Datatilsynet etter bestemmelsene i §§ ...., kan påklages til Kongen (Alternativ: Styret i Datatilsynet).

Ovenfor under avsnitt 3.6, er det diskutert hvilken myndighet Datatilsynet skal ha. Den endringen jeg foreslår i § 2, tar sikte på å skrive inn i loven det jeg konkluderte med i avsnitt 3.7.3.

Jeg er noe i tvil om hvorvidt klageadgang til Kongen skal opprettholdes, eller om det bør innføres en konstruksjon med Datatilsynet som besluttende organ - og Styret i Datatilsynet som øverste klageorgan.

Ulempen ved dette er at Datatilsynet under en slik

konstruksjon får meget stor myndighet, på et område som i vår politiske tradisjon naturlig hører under regjeringen. Det er regjeringen som til syvende og sist har det politiske ansvar for gjennomføringen av forvaltningens oppgaver. Dette taler for at regjeringen også bør ha ansvaret for innsamling, lagring og bruk av de nødvendige personopplysninger for gjennomføringen av disse oppgavene.

Det har imidlertid fra flere hold vært hevdet at Datatilsynet burde stå friere - og ha en sterkere stilling - i forhold til forvaltningen enn tilfellet er i dag. Som nevnt ovenfor under avsnitt 3.7.3, vil alltid regjeringen ha den utvei tilbake, at den kan fremme lovforslag om forhold som Datatilsynet har nedlagt forbud mot. Det er vel grunn til å tro at når Datatilsynet går til det skritt å nedlegge forbud, er saken såpass viktig at den bør "sparkes opp" på det politiske plan og diskuteres i full offentlighet i Stortinget. Jeg tror også at dette kan være et viktig "ris bak speilet", som - hvis det blir brukt - kan medvirke til at Datatilsynet blir forespurt før det settes iverk ordninger som involverer viktige personvernspørsmål.

En slik ordning forutsetter imidlertid at Datatilsynets administrasjon løsrives fra styret. Datatilsynet måtte i såfall i første instans ledes av direktøren, og avgjørelser treffes i direktørens navn. Datatilsynets styre måtte derfor bare befatte seg med forskrifter, prinsippspørsmål, og med klager over avgjørelser truffet av Datatilsynet. I utkastet til § 2 har jeg i parenteser angitt hvordan en slik ordning kan skrives inn i lovteksten.

I forbindelse med et slikt alternativ , må det vurderes om det er nødvendig med egen sekretær for styret i Datatilsynet, slik at den nødvendige uavhengigheten kan etableres i forholdet mellom førsteinstansbehandling og klagesaksbehandling. I det minste bør det være andre personer i Datatilsynets administrasjon som forbereder klagesaken, enn de som har forberedt førsteinstansvedtaket.

§ 3

<u>Uttalelse fra Datatilsynet skal være innhentet før det fremmes forslag for Stortinget eller Kongen om innsamling, lagring og bruk av personopplysninger.</u>

Uttalelse fra Datatilsynet skal være innhentet før det treffes vedtak som etter loven her er lagt til Kongen. Dette gjelder likevel ikke vedtak etter § 2.

Datatilsynet skal ellers:

1) <u>holde seg orientert om den generelle utvikling i innsamling, lagring og bruk av</u>

personopplysninger og om de problemer som knytter seg til slik innsamling,lagring og bruk. samt sørge for informasjon i denne forbindelse

2) gi råd og rettleiing om spørsmål om personvern og datasikring

3) kontrollere at de lover, forskrifter og regler som gjelder for innsamling, lagring og bruk av personopplysninger blir fulgt, og at feil eller mangler blir rettet

4) etter henvendelse eller av eget tiltak gi uttalelse i spørsmål som gjelder bruk av personopplysninger.

Kongen (Alternativ: Styret i Datatilsynet) kan gi Datatilsynet ytterligere oppgaver som gjelder innsamling, lagring og bruk m.m. av personopplysninger.

§ 3 er en bestemmelse som dels angir Datatilsynets plikter, dels angir plikt for regjeringen til å forelegge utkast til beslutninger (som skal treffes av Stortinget eller av Regjeringen) om innsamling, lagring og bruk av personopplysninger for Datatilsynet. I den nåværende loven er denne foreleggsplikten ikke helt klart uttalt, selv om det fremgår klart av lovens system og av forarbeidene at dette har vært meningen. Dett understrekes forøvrig også av Justiskomiteen i Stortinget, i forbindelse med behandlingen av Datatilsynets årsmelding for 1980. Jfr. således Innst. S. nr. 151 1981-82, s. 3, spalte 1, der det bl.a. heter:

> "Komiteen peker på at hensynet til personvernet bør være tilstrekkelig utredet og vurdert i de tilfeller hvor nye lovbestemmelser kan føre til andre resultater enn etter personregisterloven. Det er viktig at Datatilsynet får uttale seg i slike saker."

Etter min oppfatning er bestemmelsen forøvrig dekkende, og den angir Datatilsynets arbeidsområde vidt nok.

Det kan stilles spørsmålstegn ved siste ledd i bestemmelsen - ut fra hensynet til at Datatilsynet skal være "frittstående". Det vil muligens ikke være akseptabelt om Datatilsynet kan pålegges oppgaver av den regjeringen som det skal være uavhengig av. Det bør derfor overveies om ikke Styret i Datatilsynet også her bør ha forskriftsmyndigheten.

§ 4

(Foreslås opphevet)

Etter loven § 4, slik denne lyder i dag, skal Datatilsynet føre en fortegnelse over alle "registre" som det gjelder konsesjonsplikt for "etter loven § 9".

I Europarådskonvensjonen om persondatabeskyttelse (se vedlegg 4), er det en bestemmelse i artikkel 8, pkt. a), med følgende ordlyd:

> "Any person shall be enabled to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file."

Det er noe uklart hvorvidt denne bestemmelsen krever at det etableres en sentral oversikt av den typen som § 4 i personregisterloven gir anvisning på, eller om det er tilstrekkelig med regelen som står i § 7, tredje ledd. § 7 tredje ledd må i såfall utvides til også å gjelde i privat næringsvirksomhet, foreninger og stiftelser.

Formålet med fortegnelsen skulle dels være å lette Datatilsynets arbeid med å holde oversikt over registre som det gjelder konsejonsplikt for, og over hva disse registrene kan inneholde - dels å avlaste de som fører registrene for enkelthenvendelser fra å få innsyn i henhold til § 7. En slik avlastning skulle finne sted ved at de som er interessert i å benytte innsynsretten skulle kunne få en orientering om hvilke registre som er opprettet, og hvilke typer opplysninger disse inneholder ved henvendelse til Datatilsynet.

En slik bruk forutsetter for det første at de som vil bruke innsynsretten, er informert om at fortegnelsen i Datatilsynet finnes. Dernest forutsetter det at fortegnelsen dekker det overveiende antall av "registre" som det gjelder innsynsrett for etter § 7 i loven. Endelig forutsetter det at de som benytter innsynsretten vil være fornøyd med generelle opplysninger om oppbygningen av et "register", istedet for å få opplysninger om hva som er registrert om dem selv.

Etter min oppfatning vil ingen av disse forutsetningene holde. Allerede i dag er det illusorisk å tro at fortegnelsen ville gi noen oversikt som fullt ut tilfredsstiller det som var hensikten med den. Dette skyldes først og fremst at fortegnelsen ikke vil omfatte de forskriftsregulerte "registrene". Det må understrekes at det har vært svært få henvendelser for å få opplysninger fra denne fortegnelsen - men så har det heller ikke vært opplyst (informert overfor publikum) om at den skal finnes hos Datatilsynet. Det har dessuten vist seg at de fleste som har henvendt seg til Datatilsynet, har vært ute etter konkrete opplysninger om hva som er registrert om dem selv. Fortegnelsen etter § 4 inneholder ikke slike opplysninger.

I tillegg har det flere ganger vært hevdet at det ut fra beredskapshensyn ikke burde finnes noen slik sentral katalog over alle de mest sentrale og viktige personregistrene her i landet. Ytterligere et argument som har vært fremført, er at fortegnelsen vil kunne brukes som en slags "koblingskatalog" av administratorer som er ute etter bestemte opplysninger. Gjennom

fortegnelsen vil de kunne finne frem til de som har samlet inn opplysningene fra før, for så å be om kopi av opplysningene for eget formål. Dette kan være uheldig ut fra personvernhensyn.

Jeg har flere steder i denne utredningen henvist til den rivende teknologiske utviklingen. Denne utviklingen er ikke mindre rivende når det gjelder å tateknologien i bruk. Dette medfører at det vil bli stadige endringer i de beskrivelser som skal registreres i Datatilsynets fortegnelse. En meldingsordning som skal sørge for at fortegnelsen til enhver tid er ajour og korrekt, ville medføre et betydelig arbeide og byråkrati - både for de som fører personregistrene, og ikke minst for Datatilsynet. Det er dessuten grunn til å anta at det i et stort antall tilfelle ikke vil bli meldt fra til Datatilsynet om endringer - hvilket vil medføre behov for kontroll og oppfølging fra Datatilsynets side, eventuelt kombinert med straffetrussel overfor manglende meldinger.

Det er etter min oppfatning tvilsomt om nytten ved en slik fortegnelse står i forhold til kostnadene ved opprettelse og ajourhold. På denne bakgrunn foreslås § 4 opphevet.

§ 5

> Datatilsynet kan kreve de opplysninger som trengs for at det kan gjennomføre sine oppgaver. Tilsynet kan kreve å få adgang til de stedene der <u>personopplysninger</u> og tekniske hjelpemidler fins, og til å gjennomføre de prøver eller kontroller som det mener er nødvendige. <u>Den som samler inn, lagrer eller bruker personopplysningene, skal gi nødvendig bistand for at Datatilsynet skal få utført de kontroller mv. som det ønsker.</u>
>
> Datatilsynets rett til å kreve opplysninger er ikke begrenset av bestemmelser om taushetsplikt.
>
> Kongen kan gjøre slike unntak fra første og annet ledd som er nødvendig av hensyn til rikets sikkerhet.
>
> Kongen kan gi forskrift om dekning av utgiftene ved kontroll.

Stort sett gir § 5 tilstrekkelig myndighet til at Datatilsynet kan drive kontroll. Den foreslåtte endringen tar sikte på å presisere at Datatilsynet skal kunne kreve assistanse av personalet der kontrollen foretas. Slik assistanse er nødvendig, idet det aldri vil være mulig for Datatilsynet (eller noen annen organisasjon) å bygge opp en ekspertise som er istand til å kontrollere alle mulige varianter av utstyr og systemer.

Det kan være grunn til å se nærmere på unntaks-bestemmelsen i § 5, tredje ledd, første punktum. Etter denne bestemmelsen kan Kongen gjøre slike unntak fra

kontrollbestemmelsen som er nødvendige ut fra hensynet til rikets sikkerhet.

For det første er det grunn til å vurdere om det er Kongen som bør ha forskriftsmyndigheten på dette punkt. Personopplysninger som samles inn ut ifra hensynet til "rikets sikkerhet", vil det være særlige behov for å kunne vurdere, idet disse benyttes i sammenhenger og benyttes til å treffe beslutninger som har svært stor betydning for de registrerte.

Riktignok kan det hevdes at bruk av slike opplysninger er underlagt kontroll gjennom Kontrollutvalget for overvåkings- og sikkerhetstjenesten. Når man har etablert et eget organ som skal ha kontrolloppgaver overfor innsamling, lagring og bruk av personopplysninger, vil det imidlertid unektelig virke noe merkelig om dette organet ikke skulle ha befatning med en av de mest betenkelige formene for innsamling, lagring og bruk av slike opplysninger. Dessuten vil Kontrollutvalget ikke sitte inne med den samme innsikt i generelle personvernspørsmål, i det totale kontrollapparatets omfang, og sammenhengen mellom ulike deler av kontrollapparatet, som Datatilsynet vil. Datatilsynet vil på en helt annen måte enn kontrollutvalget kunne se helheten i overvåkingsproblemene.

Det er vesentlige rettssikkerhetsproblemer forbundet med overvåkingstjenestens virksomhet. Datatilsynets omdømme som kontroll- og ombudsorgan ville bli vesentlig svekket, dersom et så sentralt og viktig område ble holdt utenfor Datatilsynets område.

For overvåkings- og sikkerhetstjenesten vil det imidlertid være et sentralt poeng at så få mennesker som overhodet mulig skal få innblikk i virksomheten. Det bør derfor overveies nærmere å finne en form for koordinering av Kontrollutvalgets virksomhet med Datatilsynets kontrolloppgaver, som kan være akseptabel både for Datatilsynet og for overvåkings- og sikkerhetstjenesten. En mulig løsning ville være å ha med en representant fra Datatilsynet i Kontrollutvalget.

4.4. Endringer i kapittel 3

De endringene som foreslås i kapittel 3 i loven, må ses i lys av at jeg nedenfor foreslår kapittel 4 om konsesjonsplikt opphevet i sin helhet.

§ 6

> Innsamling, lagring og bruk av personopplysninger skal være saklig begrunnet ut fra hensynet til administrasjon og virksomhet hos den som foretar slik innsamling, lagring eller bruk.

Uten at det er nødvendig, må det ikke samles inn, lagres eller brukes

1) opplysninger om rase, eller politisk eller religiøs oppfatning

2) opplysninger om at en person har vært mistenkt, tiltalt eller dømt for straffbart forhold

3) opplysninger om helseforhold eller misbruk av rusmidler

4) opplysninger om seksuelle forhold

5) andre opplysninger om familieforhold enn slike som gjelder slektskap eller familiestatus, formuesordningen mellom ektefeller og forsørgelsesbyrde.

Bestemmelsen i § 6 inneholder det såkalte "relevansprinsippet". De endringene som er foreslått tar for det første sikte på å tilpasse bestemmelsen etter at "registerbegrepet" er tatt ut av § 1.

Videre er pkt. 2) endret. Bestemmelsen krever i sin nåværende ordlyd at det må være etablert en formell "straffesak" (at etterforskning er innledet), for at opplysningen skal anses for å være "sensitiv". Dette har ført til at det er vanskelig å reise innvendinger mot at firmaer som driver butikkontroll får opprette registre over personer som er pågrepet med ubetalte varer: Før det er innlevert anmeldelse til politiet, foreligger ingen straffesak. Den foreslåtte ordlyden utvider begrepet noe, slik at alle opplysninger om at noen har vært mistenkt, tiltalt eller dømt for straffbart forhold, anses for å være "sensitive" opplysninger.

§ 6a

Opplysninger som samles inn, lagres eller brukes for et formål, må ikke utnyttes for et annet formål, medmindre det foreligger samtykke fra den som opplysningene gjelder, eller det foreligger en særlig hjemmel i lov, for slik utnyttelse.

Bestemmelsen som er foreslått i § 6a er problematisk. Det er ikke stillet opp noe krav om at formål med innsamling av opplysninger skal fastsettes. (Se dog artikkel 5 b) i Europarådskonvensjonen om persondatabeskyttelse, der det heter at "Personal data undergoing automatic processing shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes." Jfr. også den uttalelsen som ble vedtatt av representanter for datatilsynsorganer i den vestlige verden i London høsten 1982, og som er gjengitt ovenfor under avsnitt 3.6.1.). Imidlertid følger det av bestemmelsen i § 6 at det til enhver tid skal være en saklig sammenheng mellom den

innsamling, lagring og bruk som skjer, og administrasjon og virksomhet hos den som foretar slik innsamling, lagring og bruk.

Ved en eventuell etterprøving, vil det være meget vanskelig å vurdere om den aktuelle innsamling, lagring og bruk av opplysninger er i overensstemmelse med det som opprinnelig var formålet. Dette kunne man forsøke å bøte på ved å kreve at datert formålsangivelse ble oppbevart i tilknytning til alle former for planlagt innsamling, lagring og bruk av personopplysninger.

Det er imidlertid spørsmål om slik formalisert formålsangivelse ville få noen reell betydning, idet man for det første ville få betydelige problemer med å få de ansvarlige til å etterleve bestemmelsen. Dernest ville det i løpet av kort tid, blant de som etterlever bestemmelsen, utvikle seg teknikker når det gjelder formålsangivelse som ville omfatte alle fremtidige formål som opplysningene kunne tenkes brukt til.

Som forslaget til bestemmelse står, innebærer det et generelt uttrykt prinsipp, som nok kan være noe for vagt til at det er mulig å straffesanksjonere. Likevel kan det etter min oppfatning være grunn til å uttrykke dette prinsippet i loven, som en rettesnor for de som det har adresse til. Det kan muligens gi veiledning i de åpenbare tilfellene av bruk for andre formål.

Kravet om at det skal foreligge en "hjemmel i lov" for utnyttelse til annet formål, forutsettes å kreve uttrykkelig hjemmel i formell lov. Det bør med andre ord ikke være tilstrekkelig med hjemmel i forskrift, gitt med hjemmel i lov. Dette er etter er nødvendig for å få de prinsipielt viktige sakene bragt opp til avgjørelse på et tilstrekkelig høyt politisk nivå. Dersom det aktuelle tilfellet av Datatilsynet ikke betraktes som særlig problematisk, kan Datatilsynet gi dispensasjon etter den foreslåtte bestemmelsen i § 8a.

§ 6b

Personopplysninger må ikke leveres ut, unntatt når utlevering skjer

1) med samtykke fra den opplysningen gjelder

2) til annen sammenslutning eller stiftelse innenfor eget konsern (jfr. lov av 4. juni 1976 nr. 59 om aksjeselskaper § 2-1)

3) med hjemmel i lov, eller i forskrift gitt med hjemmel i lov

4) med hjemmel i avtale mellom partene i arbeidslivet for opplysninger som vedrører medlemmer hos slik part

5) til produksjon av statistikk

6) i anonymisert form.

Overføring til, eller behandling av personopplysninger hos et databehandlingsforetak som har konsesjon etter § 22 eller hos et adresserings- eller distribusjonsforetak som har konsesjon etter § 25, regnes ikke som utlevering når dette skjer etter oppdrag fra den som er ansvarlig etter § 6c. Det samme gjelder overføring til, eller behandling av personopplysninger hos et databehandlingsforetak eller et adresserings- eller distribusjonsforetak i et annet land som har ratifisert Europarådets konvensjon om persondatabeskyttelse.

Første og annet ledd gjelder tilsvarende ved overføring av personopplysninger til utlandet.

Bestemmelsen som er foreslått i § 6b, tar sikte på å regulere adgangen til å levere ut personopplysninger. En tilsvarende bestemmelse står i dag i forskriftene til personregisterloven, § 2-1. Bestemmelsen har såvidt vites virket tilfredsstillende med henblikk på de forskriftsregulerte registrene. De tilfellene av utlevering som er regnet opp, dekker de fleste tilfelle der det foreligger legitime behov for slik utlevering.

Bestemmelsen har nær tilknytning til bestemmelsene om unntak fra taushetsplikt etter forvaltningslovens § 13 flg. Det bør derfor arbeides med en full harmonisering av reglene om unntak fra taushetsplikt, og reglene om unntak fra utleveringsforbudet etter bestemmelsen i § 6b her. Etter at "registerbegrepet" i personregisterloven § 1 er tatt bort, er det helt nødvendig at de to regelsettene er sammenfallende.

Jeg vil imidlertid understreke betydningen av at personregisterloven - i tillegg til å regulere forvaltningens innsamling, lagring og bruk av personopplysninger - også regulerer innsamling, lagring og bruk av personopplysninger i privat næringsvirksomhet, foreninger og stiftelser. Det er derfor viktig at en bestemmelse som dette blir stående i personregisterloven.

Bestemmelsen som tidligere sto i loven § 36, og som regulerte overføring av personregistre og personopplysninger til utlandet, hører etter min oppfatning systematisk hjemme i den § som regulereer utlevering av opplysninger. Etter at Norge har ratifisert Europarådskonvensjonen om persondatabeskyttelse er det ikke anledning til å ha restriksjoner på overføring av opplysninger til annet land som har ratifisert denne.

Forøvrig innebærer bestemmelsen at den som vil overføre personopplysninger til utlandet i andre tilfelle enn de som er spesifisert, må søke Datatilsynet om dispensasjon i henhold til bestemmelsene som er foreslått i § 8a.

§ 6c

Personopplysninger må ikke kobles (ved hjelp av elektroniske hjelpemidler) sammen med andre opplysninger om samme person, unntatt når koblingen

1) skjer med samtykke fra den som opplysningene gjelder

2) skjer med hjemmel i lov

3) er ledd i utveksling og sammenholding av opplysninger i et foretaks eller en institusjons vanlige administrative rutiner

4) går ut på å sammenlikne navn og adresser for å unngå dobbeltforsendelser o.l.

Bestemmelsen i § 6c tar sikte på å regulere adgangen til å foreta maskinelle sammenstillinger av opplysninger fra flere kilder om samme person. Bestemmelsen er svært lik den foreslåtte § 6b. En viktig forskjell er imidlertid at § 6c ikke bare gjelder overlevering til andre (eller innhenting fra andre) for sammenstilling, men at den også vil gjelde internt i en institusjon, en avdeling eller innenfor et foretak.

Det må imidlertid vurderes nærmere om bestemmelsen i den foreslåtte form gir tilstrekkelig rom for forskjellige alminnelige former for organisering av samlinger med personopplysninger. Jeg vil understreke meget sterkt at dersom bestemmelsen setter for snevre grenser, vil behovet for dispensasjoner fra Datatilsynet øke, hvilket igjen vil øke arbeidsbyrdene for Datatilsynet.

§ 6d

En person kan kreve sitt navn sperret mot bruk til utsendelse av direkte reklame og andre publikasjoner.

Det er etterhvert blitt svært vanlig at alle mulige abonementsregistre, medlemsregistre, kunderegistre, leverandørregistre osv., benyttes for utsendelse av direkte adressert reklame. Bestemmelsene om sletting (sperring) for utsendelse av direkte reklame slik de er etter den någjeldende loven og forskriftene, er spredd på flere forskjellige steder, og de er nokså uoversiktlige. Den forslåtte bestemmelsen tar sikte på å fastsette en generell rett for den enkelte til å kreve en samling av personopplysninger sperret mot slike utsendelser til seg. Bestemmelsen medfører at det må foretas en sanering av de någjeldende bestemmelsene (personregisterloven § 28 og § 30, jfr. forskriftene § 6-6). Det er etter min oppfatning ønskelig at denne bestemmelsen er generell. I den någjeldende loven står bestemmelsene om dette i kapitlet om adresserings- og distribusjonsvirksomhet. De langt fleste som har slike utsendelsesregistre, driver imidlertid ikke med adressering og distribusjon som

næringsvirksomhet. Det vil derfor ikke uten videre være klart for dem at tilsvarende bestemmelser gjelder for deres utsendelser.

§ 6e

Øverste administrative leder av den virksomhet der personopplysninger samles inn, lagres eller brukes, er ansvarlig for at reglene i denne loven overholdes.

Den ansvarlige må sørge for forsvarlig sikring av de personopplysninger som samles inn, lagres eller behandles, slik at ikke noen får tilgang på opplysningene uten å ha rett eller krav på dem.

Kongen (Alternativ: Styret i Datatilsynet) kan gi forskrifter om sikringstiltak for innsamling, lagring og bruk av personopplysninger, som omfattes av denne loven.

Datatilsynet kan gi pålegg som anses nødvendige for å oppnå forsvarlig sikring av bestemte opplysninger.

Den foreslåtte bestemmelsen i § 6e tar for det første sikte på å fastslå det i og for seg selvfølgelige prinsipp, at det er et ledelsesansvar å sørge for at loven overholdes.

Videre pålegges den ansvarlige å sørge for forsvarlig sikring av personopplysningene. Dette er i og for seg også en selvfølgelig plikt, men det kan være grunn til å fremheve dette spesielt, fordi det ofte synes å råde en viss uklarhet om hvem som er ansvarlig for iverksetting av sikringstiltak.

I tredje ledd i bestemmelsen er det foreslått en generell hjemmel til å gi forskrifter om sikringstiltak for innsamling, lagring og bruk av personopplysninger. Denne bestemmelsen er utformet for å avløse de noe usammenhengende hjemlene som finnes i loven i dag, og som bla. forutsetter at krav om sikringstiltak skal fastsettes individuelt for det enkelte "register"i forbindelse med konsesjonsbehandlingen. Det er grunn til å tro at dette vil kreve en betydelig arbeidsinnsats fra Datatilsynets side.

De någjeldende forskriftshjemlene er dessuten vanskelige å avpasse til det EDB-sikkerhetsdirektivet som er gitt i tilknytning til sikkerhetsinstruksen og beskyttelsesinstruksen for statsforvaltningens vedkommende. Den foreslåtte hjemmelen gjør en slik samordning vesentlig lettere.

Bestemmelsen vil etter min oppfatning kunne avløse alle de hjemlene for forskrifter om sikringstiltak som i dag

er spredd i de forskjellige kapitlene i loven.

Fjerde ledd i § 6e gir Datatilsynet hjemmel til å pålegge sikringstiltak for bestemte personopplysninger ved individuelt vedtak.

Generell kommentar

Innføringen av bestemmelser som gjengitt foran i §§ 6a - 6e, vil etter min oppfatning føre inn i loven - i svært generell form - noe av det som idag skal fastsettes i detalj av Datatilsynet under konsesjonsbehandlingen.

For at det ikke skal bli et for rigid opplegg, mener jeg imidlertid at det må være adgang til å gi dispensasjon fra disse bestemmelsene. Det bør derfor innføres en egen regel om dispensasjon, som gir en helt generell dispensasjonsadgang som skal gjelde i forhold til alle bestemmelsene i kapitlet med "alminnelige regler". Denne kommer jeg derfor tilbake til nedenfor i forbindelse med § 8.

§ 7

Alle har rett til å få opplyst hvilke opplysninger om dem selv som lagres eller bearbeides ved elektroniske hjelpemidler. Denne innsynsretten gjelder likevel ikke opplysninger som bare brukes til statistikk, forskning eller generelle planleggingsformål, eller opplysninger som registreres. Innsynsretten gjelder heller ikke opplysninger som det må anses utilrådelig at vedkommende får kjennskap til, av hensyn til personer som står dem nær.

I organ for stat eller kommune gjelder innsynsretten, slik den er avgrenset i første ledd, også for opplysninger som ikke lagres eller bearbeides ved elektroniske hjelpemidler, i den utstrekning opplysningene er lagret på en slik måte at opplysninger om den enkelte kan finnes igjen. Den som opplysningene gjelder kan likevel ikke kreve å få se dokumenter som regnes som interne etter forvaltningsloven § 18.

Alle har dessuten rett til å få opplyst hvilke samlinger av personopplysninger som føres av noen loven omfatter, og til å få opplyst hvilke typer opplysninger som er tatt inn i den enkelte samling.

Kongen (Alternativ: Styret i Datatilsynet) kan ved forskrift bestemme at det som er fastsatt i annet og tredje ledd også skal anvendes på personopplysninger som samles inn, lagres eller brukes i privat næringsvirksomhet, foreninger og stiftelser, eller for visse slike opplysninger.

Kongen (Alternativ: Styret i Datatilsynet) kan ved forskrift eller ved enkeltvedtak fastsette

flere unntak fra innsynsretten og fastsette nærmere regler eller vilkår for bruken av retten.

De endringene som er foreslått i § 7, tar sikte på å tilpasse bestemmelsen til de endringene som er foretatt i § 1 (opphevelse av registerbegrepet).

Dessuten er det innført en bestemmelse som gjør det klart at den enkelte ved henvendelse til de som loven omfatter (jfr. § 1),har krav på å få vite hvilke samlinger de har av personopplysninger, og hvilke typer opplysninger som inngår i disse samlingene. I den någjeldende loven kan det være tvil om hvorvidt den enkelte skal måtte henvise til bestemt "register" for å få vite hvilke typer opplysninger det inneholder. Bestemmelsen er dessuten utvidet til å gjelde samlinger som finnes hos private naringsdrivende, i foreninger eller stiftelser. Dette har sammenheng med den foreslåtte opphevelsen av § 4 i loven (jfr. ovenfor).

Den foreslåtte bestemmelsen løser ikke problemet med innsynsrett i det som registreres ved elektronisk tekstbehandling. Det kan være grunn til å lage et unntak fra innsynsretten for det som registreres ved elektronisk tekstbehandling, med sikte på utskrift på papir, sålenge registrering pågår. Problemet er langt på vei det samme som oppstår i forbindelse med partsinnsikt etter forvaltningsloven i "interne notater" når en sak er på forberedelsesstadiet. Tilsvarende problemstillinger vil bli berørt av den utredningen som for tiden pågår i regi av Justisdepartementet, i forbindelse med utforming av forskrifter om offentlighet av EDB-lagret informasjon i tilknytning til offentlighetsloven. Resultatet av denne utredningen vil ikke foreligge før i løpet av 1983. Spørsmålet bør behandles etter samme modell i personregisterloven som etter forskriftene til offentlighetsloven.

§ 8

Dersom en samling av personopplysninger inneholder uriktige eller ufullstendige opplysninger, opplysninger som det ikke er adgang til å ha, eller opplysninger som ikke lenger har betydning, skal opplysningene rettes, slettes eller suppleres såfremt mangelen kan få betydning for den opplysningene angår. Har mangelen ført til at det er gitt uriktige eller ufullstendige opplysninger, skal det sørges for at feilen så vidt mulig ikke får betydning for den opplysningene angår.

Når det foreligger feil som nevnt i første ledd, kan Datatilsynet gi pålegg om retting, sletting eller supplering av opplysningene og om tiltak etter første ledd annet punktum.

Bestemmelsen i § 8 kan etter min oppfatning hovedsaklig bli stående i sin opprinnelige formulering. Enkelte ord

må imidlertid endres fordi "registerbegrepet" er forlatt. Bestemmelsen gir Datatilsynet tilstrekkelig myndighet til å pålegge tiltak for å rette opp feil/ufullstendigheter i en samling av personopplysninger.

§ 8a

> Datatilsynet kan ved forskrift eller ved enkeltvedtak gjøre unntak fra bestemmelsene i dette kapittel, og fastlegge nærmere vilkår for innsamling, lagring og bruk av opplysninger som omfattes av slikt unntak.
>
> Datatilsynet kan ved forskrift eller ved enkeltvedtak nedlegge forbud mot innsamling, lagring eller bruk av personopplysninger.
>
> Datatilsynet kan ved forskrift eller enkeltvedtak fastlegge nærmere vilkår i tilknytning til innsamling, lagring eller bruk av personopplysninger.

§ 8a første ledd er innført for at bestemmelsene ikke skal bli for lite fleksible. Når det utformes forholdsnormer som setter grenser for adgang til bruk, slik som de foreslåtte §§ 6a - 6e, må det åpnes en adgang til å gjøre unntak fra reglene etter en konkret vurdering.

§ 8a annet ledd er etter min oppfatning en bestemmelse som gir Datatilsynet den nødvendige mulighet til å aksjonere mot uheldig eller ulovlig innsamling, lagring og bruk av personopplysninger.

Det kan diskuteres om det ikke ville være tilstrekkelig å falle tilbake på de alminnelige straffebestemmelsene. I såfall ville Datatilsynet være henvist til å melde eventuelle ulovligheter til politiet, med derpå følgende straffesak mot den som samler inn, lagrer eller bruker personopplysninger på ulovlige måter. Jeg mener at dette alternativet ville bli for statisk, idet det forusetter at lovens bestemmelser til enhver tid skal inneholde tilstrekkelig beskyttelse mot misbruk av personopplysninger. Den foreslåtte bestemmelse gir en mulighet for å foreta en konkret vurdering, og eventuelt til å tillate andre fremgangsmåter enn loven anviser. Dette gir etter min oppfatning en mer fleksibel ordning enn om loven skulle regnes for helt uttømmende. Politiet har mange arbeidsoppgaver, og er relativt dårlig rustet til å ta seg av saker på dette området. Sakene vil dessuten ofte ha en karakter som gjør at de blir lavt prioritert av politiet. Det er derfor ønskelig å ha sanksjonsmidler som ikke avhenger for mye av politiets medvirkning.

4.5. Endringer i kapittel 4

Kapittel 4 i loven foreslås opphevet i sin helhet. Det har i praksis vist seg at konsesjonsplikten krever såvidt mye arbeid fra de ansatte i Datatilsynet at det med dagens bemanning går ut over Datatilsynets mulighet for å ivareta personverninteressene på en tilfredsstillende måte.

Sålenge Datatilsynet ikke har ressurser til å følge opp konsesjonene ved å kontrollere at de overholdes, eller til å kontrollere at plikten til å søke konsesjoner overholdes, er det etter min oppfatning uheldig å opprettholde konsesjonsordningen.

For at konsesjonsordningen skulle kunne tjene den funksjon den opprinnelig var tiltenkt, måtte Datatilsynet vært bemannet slik at konsesjonsvedtakene kunne følges opp i praksis. For at dette skulle være mulig, måtte saksbehandlerne kunne avsette mer enn halvparten av tiden sin til kontroll-, informasjons- og oppfølgingsvirksomhet.

Med de ressurser som Datatatilynet vil råde over i de kommende år, bør derfor ambisjonsnivået trappes betydelig ned, slik at Datatilsynets oppgaver kan bli mer i overensstemmelse med de ressurser som er tilgjengelige. Etter min oppfatning utelukker dette en konsesjonsordning.

Det er vanskelig å vurdere om dette gir tilstrekkelig ivaretakelse av personverninteressene. Det kan imidlertid nokså lett konstateres at en slik ordning vil gi bedre personvern enn dagens ordning dersom Datatilsynets ressurser skal være uendret.

Samtidig finner jeg imidlertid grunn til å påpeke at det ikke ville være tale om så voldsomt store ressurser for å sette Datatilsynet istand til å opprettholde det beskyttelsesnivået for personverninteressene som den någjeldende loven legger opp til. Datatilsynets budsjett for 1983 er i overkant av kr. 3 mill. Ovenfor under avsnitt 3.7.2, er behovet for personalressurser, under en konsesjonsordning som dagens, anslått til ca. 20 personer. Dette må antas å føre til en totalutgift pr. år på ca. kr. 6 millioner til Datatilsynet. (Basert på meget grove overslag).

4.6. Endringer i kapittel 5

§ 13

> Med kredittopplysningsvirksomhet menes i kapitlet her virksomhet som består i å gi meddelelser som belyser kredittverdighet eller økonomisk vederheftighet (kredittopplysning).

Kapitlet gjelder ikke bruk av opplysninger innen et foretak eller i forhold til foretak innen samme konsern. Det gjelder heller ikke avgivelse av opplysninger til annet kredittopplysningsforetak som loven gjelder for, forutsatt at opplysningene skal brukes i dette foretakets kredittopplysningsvirksomhet.

Kongen (Alternativ: styret i Datatilsynet) kan gi utfyllende forskrift om hva som skal regnes som kredittopplysningsvirksomhet. For visse typer foretak kan Kongen (Alternativ: styret i Datatilsynet) ved forskrift eller enkeltvedtak gjøre unntak fra de enkelte bestemmelser i kapitlet.

Foretak som driver kredittopplysningsvirksomhet, kan ikke uten samtykke fra Kongen (Alternativ: styret i Datatilsynet) drive annen personopplysningsvirksomhet.

§ 13 avgrenser området for bestemmelsene om kredittopplysning. Det har skapt et visst problem i praksis at kapitlet ikke gjelder bruk av opplysninger innen et foretak eller i forhold til foretak innen samme konsern, kombinert med at kapitlet heller ikke gjelder opplysninger gitt til annet kredittopplysningsforetak som loven gjelder for. Problemet oppstår ved at en del foretak som egentlig driver annen virksomhet enn kredittopplysning (f.eks. finansiering- eller vanlig forretningsvirksomhet), søker konsesjon som kredittopplysningsforetak for å kunne motta lister med opplysninger om privatpersoner fra andre kredittopplysningsforetak. Dette er en omgåelse av loven, og bestemmelsen har vært praktisert slik av Datatilsynet, at de rene tilfelle av forsøk på omgåelser som har blitt oppdaget, har blitt nektet konsesjon.

Videre har Datatilsynet pålagt kredittopplysningsvirksomheter som mottar opplysninger om privatpersoner fra annet kredittopplysningsforetak, å sende melding til privatpersoner som det tas ut opplysninger om i firmaets øvrige virksomhet (den del av virksomheten som ikke er kredittopplysning). Det har imidlertid vist seg vanskelig for Datatilsynet å vurdere om det er forsøk på omgåelser når et firma som driver med annen virksomhet søker konsesjon som kredittopplysningsvirksomhet. Bestemmelsen slik den står i dag åpner for en viss mulighet for omgåelse, og bestemmelsen bør derfor muligens endres noe. Eventuelt kan man innføre følgende setning: "Med mindre opplysningene er innhentet fra et annet kredittopplysningsforetak", som en tilføyelse til annet punktum i første ledd av § 13. Ulempen ved dette er at første ledd i § 13 blir unødig komplisert utformet.

Det vil derfor muligens være best å la bestemmelsen stå i sin nåværende ordlyd, og legge vekt på at kapitlet gjelder fullt ut når opplysninger som overføres fra et foretak til et annet skal brukes til annet enn det mottakende foretaks kredittopplysningsvirksomhet. Det bør

ikke være anledning til å omgå reglene om kredittopplysningsvirksomhet, ved å opprette en egen avdeling som har konsesjon som kredittopplysningsforetak.

I paranteser er det ført inn et alternativ som innebærer at styret i Datatilsynet har forskriftsmyndigheten.

§ 14

> Et foretak kan ikke sette igang kredittopplysningsvirksomhet før Kongen (Alternativ: styret i Datatilsynet) har gitt samtykke til det.
>
> Ved avgjørelsen av om det skal gis samtykke, skal det legges vekt på om virksomheten kan forutsettes å ville bli drevet på en redelig og forsvarlig måte. Innenfor rammen av bestemmelsene i denne lov kan det settes slike vilkår for konsesjonen som er egnet til å fremme disse formål, bl.a. om sikkerhet for ansvar. For foretak som utenlandske interesser har bestemmende innflytelse over, kan det settes vilkår som gjelder etableringsformen og sammensetningen av selskapets ledelse.

Bestemmelsene om konsesjonsplikt for kredittopplysningsforetak har ikke skapt nevneverdige problemer for Datatilsynet. Antallet konsesjonssaker er heller ikke så stort at en opprettholdelse av konsesjonsplikten vil skape nevneverdige problemer.

Det har vist seg at det er relativt uryddige forhold innenfor en del av kredittopplysningsbransjen. Det synes derfor å være god grunn til å opprettholde en konsesjonsplikt, som innebærer at Datatilsynet opprettholder den formen for kontroll med virksomheten som konsesjonsplikten innebærer.

Den eneste forandring som foreslås i denne bestemmelsen, er derfor at konsesjonsmyndigheten legges til styret for Datatilsynet.

§ 15

> Kredittopplysningsforetaket skal påse at de opplysninger som brukes i kredittopplysningsøyemed så vidt mulig er fullstendige, og at det ikke brukes opplysninger som kan danne grunnlag for ugrunnet eller urimelig avvisende holdning til den opplysningene gjelder.
>
> En opplysning som ved kalenderårets utgang vil være 5 år gammel eller mer, kan bare brukes dersom det er åpenbart at forholdet fortsatt har vesentlig betydning for vurderingen av den opplysningene gjelder.

§ 15 har ikke medført spesielle problemer. Det kan

eventuelt vurderes om 5-årsfristen i annet ledd er noe for lang, slik at det f.eks bør være en 3-årsfrist for de aktuelle opplysningene.

§ 16

> Foretaket kan ikke som ledd i kredittopplysningsvirksomhet bruke:
>
> 1) Opplysninger om rase, eller politisk eller religiøs oppfatning
>
> 2) Opplysninger om at en person har vært mistenkt, tiltalt eller dømt <u>for straffbart forhold</u>
>
> 3) Opplysninger om helseforhold eller misbruk av rusmidler
>
> 4) Opplysninger om seksuelle forhold
>
> 5) Andre opplysninger om familieforhold enn slike som gjelder slektskap eller familiestatus, formuesordningen mellom ektefeller og forsørgelsesbyrde.
>
> Kongen (<u>Alternativ: styret i Datatilsynet</u>) kan likevel gi samtykke til at opplysninger som nevnt i første ledd nummer 2 og 3 samles inn og meddeles i visse tilfelle.

I denne bestemmelsen er det foreslått en endring i overensstemmelse med den endringen som er foreslått i § 6 i loven. Jfr. om dette fremstillingen ovenfor under avsnitt 4.4.

§ 17

> Kredittopplysning må ikke gis når det etter det som foreligger, går frem at bestilleren ikke har saklig behov for den.
>
> Kongen (<u>Alternativ: styret i Datatilsynet</u>) kan ved forskrift eller for det enkelte foretak gi regler om beskyttelse av innsamlede opplysninger mot uberettiget bruk.

Annet ledd i § 17 gir en hjemmel til å gi forskrifter om sikringstiltak. Etter den foreslåtte § 6 e i lovens kapittel 3, (jfr. ovenfor under avsnitt 4.4) vil det foreligge en tilstrekkelig hjemmel til å gi forskrifter om sikringstiltak også for opplysninger som samles inn i kredittopplysningsvirksomhet. Det er derfor ikke nødvendig å ha med bestemmelsen i annet ledd i § 17. Denne kan derfor sløyfes.

§ 18

> Kredittopplysning skal vanligvis meddeles skriftlig. Den kan gis muntlig dersom den ikke

inneholder noe som kan bli anført mot den opplysningen gjelder, eller kredittopplysningen av praktiske grunner må gis uten opphold. Blir en kredittopplysning gitt muntlig, skal opplysningens innhold samt bestillerens navn og adresse noteres og oppbevares minst et halvt år. Inneholder den noe som kan bli anført mot den opplysningen gjelder, skal den bekreftes skriftlig.

Kredittopplysninger kan gis ved utsending av publikasjoner eller lister, forutsatt at publikasjonen eller listen bare inneholder opplysninger om næringsdrivende, og at opplysningene er gitt i summarisk form. Slike publikasjoner kan bare sendes til medlemmer og abonnenter.

Anmodning om at kredittopplysning som går ut på at bestilleren skal få vite det kredittopplysningsforetaket blir kjent med i fremtiden eller i et bestemt tidsrom, kan bare omfatte opplysninger om næringsdrivende.

Kredittopplysninger kan gis ved terminaltilknytning til kredittopplysningsforetakets samling (database e.l.) av opplysninger. Utsending av kredittopplysninger via terminal kan bare omfatte opplysninger om næringsdrivende.

§ 18 i den någjeldende loven bygger på at kredittopplysninger som gis i form av masseopplysninger, blir gitt i trykte bøker, på microfilmkort e.l. Det er imidlertid bare et spørsmål om tid før det blir organisert databaser for kredittopplysningsvirksomhet, der abonnenter kan spørre på kredittopplysningen direkte fra terminal, som enten kan være fast tilkoblet, eller som kan være basert på oppringt samband.

Bestemmelsen i § 18 i den någjeldende lov passer dårlig for dette tilfellet. Bl.a. er det vanskelig å si at et firma som spør på en og en person i et slikt databaseopplegg innhenter masseopplysninger. Det er derfor nødvendig med en tilføyelse til § 18, som gjør det klart at opplysninger som gjøres tilgjengelige via terminaltilknytning, bare må omfatte opplysninger om næringsdrivende.

I tilknytning til bestemmelsene i § 18 kan det være grunn til å nevne at bransjen har betydelige problemer med å skille mellom næringsdrivende og privatpersoner. Dette har medført at virksomhetene i tvilstilfelle har vært nødt til å holde personer som de ikke kan få stadfestet er næringsdrivende utenfor publikasjoner og lister. Videre har de vært nødt til å sende gjenpart av kredittopplysninger som er gitt om slike personer, til personene selv.

Det finnes i Norge en del registre som til en viss grad

kan antyde hvor vidt noen er næringsdrivende eller privatpersoner. Således har vi arbeidsgiver- og arbeidstakerregisteret, merverdiavgiftsregisteret, og firmaregistre. I Statistisk sentralbyrå har vi videre et bedrifts- og foretaksregister. Det bør muligens gjøres et arbeid i Norge med å innføre en sanering og samordning av de oversiktene av forskjellig slag som finnes over næringsdrivende/arbeidsgivere. I denne sammenheng kan nevnes at man i Sverige har innført et "fødselsnummer" for bedrifter og foretak, og at det er opprettet et sentralt foretaksregister.

Dette spørsmålet går muligens noe utenfor rammen av denne utredningen. Siden de fleste kredittopplysningsforetak får masseopplysninger fra løsøreregisteret i Brønnøysund, ville det imidlertid være en fordel om dette registeret kunne skille klart mellom opplysninger om næringsdrivende og opplysninger om privatpersoner. Uklarhetene fører til at det er vanskelig i praksis å etterleve reglene i § 18.

§ 19

> Når kredittopplysning om noen som ikke er næringsdrivende blir gitt eller bekreftet skriftlig, skal kredittopplysningsforetaket vederlagsfritt sende gjenpart, kopi eller annen melding om innholdet til den som det er bestilt opplysninger om. Foretaket plikter ikke i en slik gjenpart, kopi eller annen melding å opplyse hvem som har bestilt opplysningene, eller hvem det har mottatt opplysningene fra.

Også i den nägjeldende lovens § 19 er det tatt inn en regel om at foretaket ikke plikter å opplyse kilden for sine opplysninger, eller hvem det har gitt opplysninger til. Denne bestemmelsen kan i hovedsak opprettholdes i § 19. I § 20 nedenfor, vil det imidlertid bli foreslått at et foretak etter forespørsel skal ha plikt til å oppgi slik kilde. Dette er årsaken til at bestemmelsen i § 19 er foreslått begrenset til de tilfelle hvor kredittopplysningsforetaket sender gjenpart, kopi eller annen melding om innholdet til ikke næringsdrivende, som det blir gitt opplysning om. Se nærmere om begrunnelsen nedenfor i tilknytning til § 20.

§ 20

> Alle har rett til å få opplyst hva foretaket har lagret om dem selv til bruk i kredittopplysningsøyemed, og til å få opplyst hvilke kredittopplysninger som er gitt om dem de siste seks måneder. Svar skal gis skriftlig om ikke vedkommende har samtykket i at det blir gitt på annen måte. Blir opplysning om hva et foretak har lagret gitt i form av et sammendrag, eller har foretaket lagret opplysninger som ikke gjengis fullstendig, skal dette sies i svaret. Den opplysningene gjelder, kan kreve å få gjennomgå alle dokumenter m.m. ved henvendelse til foretaket.

> Foretaket plikter etter forespørsel fra den det er gitt opplysninger om å opplyse hvem som har bestilt opplysningene, og hvem det har mottatt opplysningene fra.
>
> Foretaket kan beregne seg en rimelig godtgjørelse når opplysning etter første ledd blir gitt skriftlig.

Den nägjeldende § 19 og 20 inneholder bestemmelser som sier at en omspurt person ikke har anledning til å få vite kilden for opplysningene, og heller ikke ha rett til å få vite hvem som har mottatt kredittopplysninger. I forarbeidene er det ikke gitt noen begrunnelser for dette, utover at det i Ot.prp. nr. 2 1977-78, side 92 står at det fra rettssikkerhetssynspunkt neppe kan reises avgjørende innvendinger mot disse løsningene.

Tilsvarende bestemmelser i den danske og den svenske loven inneholder en mulighet for den det er gitt feilaktige opplysninger om, til å få vite både kilder og adressater for opplysninger.

§ 40 i loven statuerer et objektivt erstatningsansvar for kredittopplysningsvirksomhet som har meddelt opplysninger i strid med bestemmelser gitt i eller i medhold av loven, eller som har meddelt opplysninger som viser seg uriktige eller åpenbart misvisende. Etter min oppfatning er denne erstatningsbestemmelsen illusorisk, dersom den det er gitt opplysninger om ikke har anledning til å gjøre seg kjent med hvor opplysningene stammer fra, og hvem som har mottatt slike feilaktige opplysninger. På denne bakgrunn bør bestemmelsen i § 20 annet ledd forandres som foreslått ovenfor, slik at det uttrykkelig sies at et foretak plikter å opplyse både hvem som har bestilt opplysninger, og hvem som har mottatt opplysninger, på begjæring fra den opplysningene gjelder.

§ 21

> Kongen (Alternativ: styret i Datatilsynet) kan ved forskrift fastsette at § 14 om konsesjonsplikt skal gjelde også for andre foretak som driver personopplysningsvirksomhet. I konsesjonen kan det settes vilkår om innsamling, lagring og bruk av opplysningene, samt om kontroll, om innsynsrett for den opplysningene gjelder og om rett til å kreve seg slettet fra slik samling av opplysninger.

Det har foreløpig ikke vært nødvendig å gi forskrifter i medhold av § 21. Dersom "Kirsten giftekniv"-virksomhet ved hjelp av datamaskiner blir særlig mer utbredt, og dersom detektivbyråvirksomhet eller headhuntingvirksomhet blir mer utbredt, kan dette bli aktuelt. Bestemmelsen gir imidlertid tilstrekkelige fullmakter i dag. Det bør imidlertid også her overveies å overlate forskriftsmyndigheten til Datatilsynets styre.

4.7. Endringer i kapittel 6

§ 22

> Virksomhet som består i å bearbeide personopplysninger for andre ved elektroniske hjelpemidler, må ikke settes i gang før Kongen (Alternativ: Styret i Datatilsynet) har gitt samtykke til det. § 14 annet ledd gjelder tilsvarende.
>
> Første ledd gjelder ikke dersom bearbeidelsen utelukkende skjer for andre foretak innen samme konsern. Det gjelder heller ikke dersom bearbeidelsen utelukkende skjer for over-, under-, eller sideordnede forvaltningsorganer innenfor en statlig eller kommunal etat, eller når et forvaltningsorgan bearbeider opplysninger for kollegiale organer, sakkyndige eller tilsynsførere mv. som er tilknyttet etaten, eller for private som er engasjert for å løse oppgaver for etaten.
>
> Kongen (Alternativ: Styret i Datatilsynet)kan gi utfyllende forskrifter om hva som skal reknes som databehandlingsforetak ved anvendelse av første ledd, og kan ved forskrift eller enkeltvedtak gjøre unntak fra de enkelte bestemmelser i dette kapitlet.

Også konsesjonsplikten for databehandlingsforetakene kan med fordel opprettholdes. Den vil bidra til at Datatilsynet kan opprettholde kontakt med, og oversikt over en bransje som er svært sentral i forhold til innsamling, lagring og bearbeiding av personopplysninger.

I Odelstingsproposisjon nr. 2 1977 - 78 var det foreslått at kapitlene 5, 6, 7 og 8 bare skulle gjelde for privat næringsvirksomhet, foreninger eller stiftelser (med andre ord ville kredittopplysning, databehandling, adressering eller markeds-og opinionsundersøkelser som ble drevet av organer for stat og kommune, ikke være konsesjonspliktig virksomhet - og de særlige materielle reglene for slike virksomheter ville ikke få anvendelse). Dette ble forand ret i Stortinget da loven ble vedtatt, slik at kapittel 5-8 gjelder også når slike virksomheter blir drevet av organer for stat og kommune.

I den någjeldende loven er foretak som utelukkende bearbeider personopplysninger for andre foretak innenfor samme konsern, fritatt fra konsesjonsplikt (personregisterloven § 22 annet ledd). Med den endringen som ble foretatt i Stortinget, ble det ikke gjort noen tilsvarende endring som innebar konsesjonsfritak for bearbeiding innenfor en konsernliknende sammensetning av forvaltningsorganer. Konsernbegrepet passer ikke i organer for stat og kommune. Da personregisterloven ble satt iverk, ble det derfor laget en bestemmelse i

forskriftene § 5-1, som tilsvarer den forandringen som her er foreslått i § 22. Endringen tar sikte på lovfeste et tilsvarende unntak fra konsesjonsplikten for organer for stat og kommune, som vi i dag har innenfor konserner.

§ 23

> Foretak som må ha konsesjon etter § 22 første ledd, må ikke uten avtale med oppdragsgiveren anvende opplysningene til andre formål enn det oppdraget gjelder. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse.

Bestemmelsene i § 23 er svært sentrale for en redelig og forsvarlig databehandlingsvirksomhet. Bestemmelsene har nær sammenheng med eventuelle bestemmelser som vil bli gitt om såkalt "datakriminalitet". Bestemmelsen i § 23 er et straffesanksjonert forbud mot kopiering eller misbruk av personopplysninger.

Bestemmelsen bør etter min oppfatning bli stående i personregisterloven selv om det skulle bli gitt bestemmelser i straffeloven som innebærer forbud mot kopiering/utnyttelse av opplysninger som lagres ved elektroniske hjelpemidler. Bestemmelsen i personregisterloven på dette punkt bør imidlertid vurderes i sammenheng med de bestemmelser som etter all sannsynlighet vil bli foreslått om datakriminalitet.

§ 24

> Foretaket skal treffe de sikringstiltak som trengs.
>
> Kongen (Alternativ: styret i Datatilsynet) kan ved forskrift eller for det enkelte foretak gi bestemmelser om de sikringstiltak som skal gjennomføres.

I § 24 i den någjeldende personregisterloven, er det i annet ledd gitt fullmakt til å gi forskrift, eller treffe enkeltvedtak med bestemmelser om sikringstiltak som skal gjennomføres av et databehandlingsforetak. Denne forskriftshjemmelen er foreslått opprettholdt i utkastet ovenfor. På samme måte som for den tilsvarende hjemmelen i tilknytning til kredittopplysningesvirksomhet (jfr. § 17 ovenfor), kan det imidlertid overveies om ikke den nødvendige hjemmelen nå vil finnes i utkastet til § 6 e. I såfall kan hjemmelen i § 24 annet ledd sløyfes.

4.8. Endringer i kapittel 7

Bestemmelsene om adresserings- og distribusjonsvirksomhet, slik de i dag står i kapittel 7 i loven, og i forskriftenes kapittel 6, synes å virke tilfredsstillende. Jeg ser derfor ingen grunn til å foreslå at det foretas endringer i bestemmelsene i dette kapitlet i

loven.

Det må imidlertid overveies i dette kapitlet - på samme måte som foreslått i de øvrige kapitlene - om myndigheten etter loven til å treffe enkeltvedtak, eller forskrift bør legges til styret i Datatilsynet.

Bestemmelsene i § 26, 27 og 28 må dessuten endres for å tilpasse dem til opphevelsen av "registerbegrepet".

Videre må det også i dette kapitlet vurderes om ikke hjemmelen til å gi regler om sikring (i § 29) kan oppheves, idet det må antas at den generelle hjemmelen for å gi sikringsforskrifter som foreslås i § 6e vil være dekkende.

4.9. Endringer i kapittel 8

Heller ikke bestemmelsene i kapittel 8 har hittil skapt nevneverdige problemer. Også her må det overveies om forskriftsmyndighet og enkeltvedtaksmyndighet bør legges til styret i Datatilsynet.

§ 33 må tilpasses opphevelsen av "registerbegrepet", og det må overveies om hjemmelen i § 34 til å gi sikringsregler mv. er overflødig, som en følge av innføringen av den generelle hjemmelen i § 6e.

Det er et begrenset antall foretak som driver slik virksomhet, og virksomheten kan i visse tilfelle innebære at det samles inn opplysninger som er av sensitiv karakter. Bransjen har selv på dette området utformet et sett med etiske regler, som de besørger etterfulgt ved en selvjustis innenfor norsk markedsanalyseforening. Siden ikke alle firmaer i bransjen er medlemmer av denne foreningen, er det etter min oppfatning grunn til å opprettholde reglene i personregisterloven på dette punktet.

4.10. Endringer i kapittel 9

§ 36 om overføring av opplysninger til utlandet, foreslås opphevet i sin helhet. En bestemmelse om overføring eller utlevering av opplysninger til utlandet er tatt inn i § 6 b i loven. Bestemmelsen nører etter min oppfatning systematisk hjemme i tilknytning til den alminnelige bestemmelsen om utlevering av opplysninger. Jeg henviser således til fremstillingen i tilknytning til § 6 b ovenfor under avsnitt 4.4.

§ 37

> Kongen (Alternativ: styret i Datatilsynet) kan gi forskrift om samarbeid mellom Datatilsynet og tilsynsmyndigheter i andre land. I slik forskrift kan det fastsettes særlige regler om meldeplikt for overføring av personopplysninger

og om kontroll med eller tilintetgjøring av opplysninger.

§ 37 om samarbeid med tilsynsmyndigheter i andre land, foreslås bare endret for å tilpasse bestemmelsen til opphevelsen av registerbegrepet.

Siden dette blir den eneste bestemmelsen som står igjen i kapittel 9, kan det være grunn til å endre overskriften på kapitlet til å lyde: "Samarbeid med tilsynsmyndigheter i andre land."

4.11. Endringer i kapittel 10

De enkelte paragrafer i kapitlene 3 til 9 må gjennomgås med tanke på å knytte straffebestemmelser til de enkelte reglene som er fastsatt. Hver enkelt bestemmelse må vurderes ut fra legalitetsprinsippets krav til straffesanksjonerte materielle regler (jfr. ovenfor under avsnitt 3.3).

Etter min oppfatning er de strafferammer og erstatningsregler som er satt i kapittel 10 i loven for øvrig tilstrekkelige.

4.12. Endringer i kapittel 11

§ 41 i loven kan oppheves, idet § 3 første ledd vil ivareta behovet for kontroll med ivaretakelse av personverninteressene for registre som opprettes ved egen lov, og for registre som opprettes ved regjeringsbeslutning. Dessuten vil slike registre fullt ut være underlagt de reglene som står i kapittel 3 i loven, med mindre vedkommende regjeringsbeslutning eller lovvedtak bestemmer noe annet.

Ikrafttredelse av endringer som foreslått i denne utredningen, må vurderes særskilt. Særlig må det vurderes hvorledes endringene skal gjelde i forhold til registre som pr. i dag har fått konsesjon. Antakelig bør de nye reglene avløse de konsesjoner som er gitt. Likeledes må reglene avløse de regler som i dag er gitt i forskriftene til personregisterloven for forskjellige typer registre. I forbindelse med gjennomføring av en eventuell endring i tråd med det som her er foreslått, må det derfor satses betydelige midler på en informasjonskampanje overfor de som har fått konsesjoner, overfor de som har registre regulert ved forskrifter, og overfor de som har samlinger med personopplysninger som reguleres av den foreslåtte ordningen. I en slik kampanje må det legges særlig stor vekt på å få frem at det ikke er meningen å svekke kontrollen med innsamling, lagring og bruk av personopplysninger i forhold til det som foregår i dag. En slik kontroll er i dag mer viktig enn noensinne

VEDLEGG 1: Lov av 9.6.1978 nr. 48 om personregistre mm.

KAPITTEL 1 Lovens område

§ 1

Loven gjelder for personregistre og for annen bruk av personopplysninger i visse typer virksomhet.

Med personopplysninger er ment opplysninger og vurderinger som direkte eller indirekte kan knyttes til identifiserbare enkeltpersoner, sammenslutninger eller stiftelser. Med personregistre er ment registre, fortegnelser m.m. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte person kan finnes igjen.

Loven gjelder for personregistre og bruk av personopplysninger i organ for stat eller kommune og i privat næringsvirksomhet, foreninger eller stiftelser.

Kongen kan bestemme at loven ikke skal gjelde for visse typer personregistre.

KAPITTEL 2 Datatilsynet

§ 2

Det blir opprettet et datatilsyn. Datatilsynet skal være et frittstående organ underordnet Kongen og det departementet Kongen fastsetter.

Datatilsynet blir ledet av et styre, som skal ha 7 medlemmer.

Medlemmene blir oppnevnt av Kongen, som også fastsetter hvem som skal være styrets formann og nestformann.

§ 3

Uttalelse fra Datatilsynet skal være innhentet før det blir gjort vedtak som i loven er lagt til Kongen. Dette gjelder likevel ikke vedtak etter § 2.

Datatilsynet skal ellers :

1) holde seg orientert om den generelle utvikling i bruken av personregistre og om de problemer som knytter seg til slike registre, samt sørge for informasjon i denne forbindelse,

2) gi råd og rettleiing om spørsmål om personvern og datasikring til dem som planlegger å opprette personregistre,

3) kontrollere at lover, forskrifter og regler som

gjelder for personregistre, blir fulgt, og at feil eller mangler blir rettet,

4) etter henvendelser eller av eget tiltak gi uttalelse i spørsmål som gjelder bruk av personopplysninger.

Kongen kan gi Datatilsynet ytterligere oppgaver som gjelder bruk m.m. av personopplysninger ellers.

§ 4

Datatilsynet skal føre en systematisk fortegnelse over personregistre som det gjelder konsesjonsplikt for etter § 9. Fortegnelsen skal vise hvem som har ansvar for registeret, hvilke typer opplysninger registeret kan inneholde, og hva det kan brukes til. Fortegnelsen skal henvise til de regler som ellers er fastsatt etter § 11 Et eksemplar av reglene skal oppbevares av Datatilsynet.

Fortegnelsen skal være tilgjengelig for alle.

Kongen kan gi nærmere regler om fortegnelsen og gjøre slike unntak fra første ledd som er nødvendige ut fra beredskapshensyn eller hensynet til rikets sikkerhet.

§ 5

Datatilsynet kan kreve de opplysninger som trengs for at det kan gjennomføre sine oppgaver. Tilsynet kan kreve å få adgang til de stedene der personregistre og tekniske hjelpemidler fins, og til å gjennomføre de prøver eller kontroller som de mener er nødvendige.

Datatilsynets rett til å kreve opplysninger er ikke begrenset av bestemmelser om taushetsplikt.

Kongen kan gjøre slike unntak fra første og annet ledd som er nødvendige av hensyn til rikets sikkerhet. Kongen kan også gi forskrift om dekning av utgiftene ved kontroll.

KAPITTEL 3 Alminnelige regler

§ 6

Registrering av personopplysninger skal være saklig begrunnet ut fra hensynet til administrasjon og virksomhet i det organ eller foretak som foretar registreringen.

Uten at det er nødvendig, må det ikke registreres

1. opplysninger om rase, eller politisk eller religiøs oppfatning,
2. opplysninger om at en person har vært mistenkt, tiltalt eller dømt i straffesak.
3. opplysninger om helseforhold eller misbruk av midler,
4. opplysninger om seksuelle forhold,
5. andre opplysninger om familieforhold enn slike som gjelder slektskap eller familiestatus, formuesordningen mellom ektefeller og forsørgelsesbyrde.

§ 7

Alle har rett til å få opplyst hvilke opplysninger om dem selv som lagres eller bearbeides ved elektroniske hjelpemidler. Denne innsynsretten gjelder likevel ikke registre som bare brukes til statistikk, forskning eller generelle planleggingsmål. Innsynsretten gjelder heller ikke opplysninger som det må anses utilrådelig at vedkommende får kjennskap til, av hensyn til deres helse eller forholdet til personer som står dem nær.

For personregistre i organ for stat eller kommune gjelder innsynsretten, slik den er avgrenset i første ledd, også for opplysninger som ikke lagres eller bearbeides ved elektroniske hjelpemidler. Den registrerte kan likevel ikke kreve å få se dokumenter som regnes som interne etter forvaltningslovens § 18.

For personregistre i organ for stat eller kommune har alle dessuten rett til å få opplyst hvilke typer opplysninger som er tatt inn i registeret.

Kongen kan ved forskrift bestemme at det som er fastsatt i annet og tredje ledd, også skal anvendes på personregistre i privat næringsvirksomhet, foreninger eller stiftelser, eller for visse slike registre.

Kongen kan ved forskrift eller for det enkelte register fastsette flere unntak fra innsynsretten og fastsette nærmere regler eller vilkår for bruken av retten.

§ 8

Dersom et personregister inneholder uriktige eller ufullstendige opplysninger, opplysninger som det ikke er adgang til å ta inn i registeret, eller opplysninger som ikke lenger har betydning, skal opplysningene rettes, slettes eller suppleres såframt mangelen kan få betydning for den registrerte. Har mangelen ført til at det er gitt uriktige eller ufullstendige opplysninger, skal det sørges for at feilen så vidt mulig ikke får betydning for den registrerte.

Når det foreligger feil som nevnt i første ledd, kan Datatilsynet gi pålegg om retting, sletting eller supplering av registeret og om tiltak etter første ledd annet punktum.

KAPITTEL 4 Plikt til å søke samtykke til å opprette personregistre

§ 9

Det kreves samtykke fra Kongen (konsesjon) for å opprette personregistre som skal gjøre bruk av elektroniske hjelpemidler. Slikt samtykke kreves også for å opprette andre personregistre dersom de skal inneholde

1) opplysninger om rase, eller politisk eller religiøs oppfatning
2) opplysninger om at en person har vært mistenkt, tiltalt eller dømt i straffesak

3) opplysninger om helseforhold eller misbruk av rusmidler
4) opplysninger om seksuelle forhold eller
5) andre opplysninger om familieforhold enn slike som gjelder slektskap eller familiestatus, formuesordningen mellom ektefeller og forsørgelsesbyrde.

Kongen kan bestemme at visse typer personregistre skal være unntatt fra konsesjonsplikten etter første ledd. For slike registre kan det fastsettes forskrifter om forhold som er nevnt i § 11. Det kan også fastsettes andre forskrifter for å begrense de problemer registeret ellers kunne medføre for den enkelte, bl.a. regler om at registeret skal kontrolleres av Datatilsynet og tas med i fortegnelsen etter § 4.

Kongens myndighet etter første og annet ledd kan bare delegeres til departementet eller til Datatilsynet.

Kongen kan gi forskrifter om sikringstiltak ved anlegg for drift av personregistre som nevnt i første ledd.

§ 10

Ved avgjørelsen av om samtykket skal gis, skal det - innenfor den rammen som er fastsatt i § 6 - vurderes om opprettelse og bruk av personregisteret kan volde problemer for den enkelte som ikke kan løses tilfredsstillende ved regler etter § 11. Dersom slike problemer kan oppstå, må det overveies om de blir oppveid av hensyn som taler for at registeret blir opprettet.

§ 11

Når det blir gitt samtykke etter § 9, skal det fastsettes regler for personregisteret som angir hvilke typer opplysninger registeret kan benyttes til.

I reglene skal det dessuten fastsettes slike vilkår som har betydning for bruken av registeret eller kan begrense de ulempene opprettelsen og bruken av registeret ellers kunne medføre. Særlig skal det overveies å fastsette regler om

1) innsamling og kontroll av de opplysninger registeret kan inneholde
2) behandling og lagring av disse opplysningene
3) adgangen til samkjøring med andre personregistre (kobling)
4) bruk av personnummer
5) utlevering av opplysninger, bl.a. om opplysninger kan overføres til andre registre
6) omfanget og innholdet av den informasjon som skal gis ved meldinger eller andre henvendelser til den registrerte
7) den enkeltes rett til å kreve opplysninger etter § 7
8) retting av opplysninger og rutiner i registeret
9) ajourføring av registeret
10) sletting eller ikke-bruk av opplysninger etter en viss tid, og eventuelt overføring av registeret til arkivverket.

Reglene skal dessuten peke ut det organ eller foretak eller den person som har ansvaret for at reglene blir gjennomført.

§ 12

Regler som er fastsatt etter § 11, kan ikke fravikes uten at det er innhentet samtykke fra det organet som fastsetter reglene, eller - når reglene bestemmer det - fra departementet eller Datatilsynet.

KAPITTEL 5 Kreditt- og personopplysningsvirksomhet

§ 13

Med kredittopplysningsvirksomhet menes i kapitlet her virksomhet som består i å gi meddelelser som belyser kredittverdighet eller økonomisk vederheftighet (kredittopplysning). Kapitlet gjelder ikke bruk av opplysninger innen et foretak eller i forhold til foretak innen samme konsern. Det gjelder heller ikke avgivelse av opplysninger til annet kredittopplysningsforetak som loven gjelder for, forutsatt at opplysningene skal brukes i dette foretakets kredittopplysningsvirksomhet.

Kongen kan gi utfyllende forskrift om hva som skal regnes som kredittopplysningsvirksomhet. For visse typer foretak kan Kongen ved forskrift eller enkeltvedtak gjøre unntak fra de enkelte bestemmelser i kapitlet.

Foretak som driver kredittopplysningsvirksomhet, kan ikke uten samtykke fra Kongen drive annen personopplysnings- virksomhet.

§ 14

Et foretak kan ikke sette i gang kredittopplysnings- virksomhet før Kongen har gitt samtykke til det.

Ved avgjørelsen om at det skal gis samtykke, skal det legges vekt på om virksomheten kan forutsettes å ville bli drevet på en redelig og forsvarlig måte. Innenfor rammen av bestemmelsene i denne lov kan det settes slike vilkår for konsesjonen som er egnet til å fremme disse formål, bl.a. om sikkerhet for ansvar. For foretak som utenlandske interesser har bestemmende innflytelse over, kan det settes vilkår som gjelder etableringsformen og sammensetningen av selskapets ledelse.

§ 15

Kredittopplysningsforetaket skal påse at de opplysninger som brukes i kredittopplysningsøyemed, så vidt mulig er fullstendige, og at det ikke brukes opplysninger som kan danne grunnlag for ugrunnet eller urimelig avvisende holdning til den opplysningene gjelder.

En opplysning som ved kalenderårets utgang vil være 5 år gammel eller mer, kan bare brukes dersom det er åpenbart at forholdet fortsatt har vesentlig betydning for vurderingen av den opplysningene gjelder.

§ 16

Foretaket kan ikke som ledd i kredittopplysnings- virksomhet bruke

1) opplysninger om rase, eller politisk eller religiøs oppfatning
2) opplysninger om at en person har vært mistenkt, tiltalt eller dømt i straffesak
3) opplysninger om helseforhold eller misbruk, av rusmidler
4) opplysninger om seksulle forhold
5) andre opplysninger om familieforhold enn slike som gjelder slektskap eller familiestatus, formuesordningen mellom ektefeller og forsørgelsesbyrde.

Kongen kan likevel gi samtykke til at opplysninger som er nevnt i første ledd nr. 2 og 3 samles inn og meddeles i visse tilfelle.

§ 17

Kredittopplysning må ikke gis når det etter det som foreligger, går fram at bestilleren ikke har saklig behov for den.

Kongen kan ved forskrift eller for det enkelte foretak gi regler om beskyttelse av innsamlede opplysninger mot uberettiget bruk.

§ 18

Kredittopplysning skal vanligvis meddeles skriftlig. Den kan gis muntlig dersom den ikke inneholder noe som kan bli anført mot den opplysningen gjelder, eller kredittopplysningen av praktiske grunner må gis uten opphold. Blir en kredittopplysning gitt muntlig, skal opplysningens innhold samt bestillerens navn og adresse noteres og oppbevares minst et halvt år. Inneholder den noe som kan bli anført mot den opplysningen gjelder, skal den bekreftes skriftlig.

Kredittopplysninger kan gis ved utsending av publikasjon eller lister, forutsatt at publikasjonen eller listen bare inneholder opplysninger om næringsdrivende, og at opplysningene er gitt i summarisk form. Slike publikasjoner kan bare sendes til medlemmer og abonnenter.

Anmodning om kredittopplysning som går ut på at bestilleren skal få vite det kredittopplysningsforetaket blir kjent med i framtiden eller i et bestemt tidsrom, kan bare omfatte opplysninger om næringsdrivende.

§ 19

Når kredittopplysning om noen som ikke er næringsdrivende blir gitt eller bekreftet skriftlig, skal kredittopplysningsforetaket vederlagsfritt sende gjenpart, kopi eller annen melding om innholdet til den det er bestilt opplysninger om. Foretaket plikter ikke å opplyse hvem som har bestilt opplysningene, eller hvem det har mottatt opplysningene fra.

§ 20

Alle har rett til å få opplyst hva foretaket har lagret om dem selv til bruk i kredittopplysningsøyemed, og til å få opplyst hvilke kredittopplysninger som er gitt om dem de siste seks måneder. Svar skal gis skriftlig om ikke vedkommende har samtykket i at det blir gitt på annen måte, eller har foretaket lagret opplysninger som ikke gjengis fullstendig, skal dette sies i svaret. Den opplysningene gjelder, kan kreve å få gjennomgå alle dokumenter m.m. ved henvendelse til foretaket.

Foretaket plikter ikke å opplyse hvem som har bestilt opplysningene fra.

§ 21

Kongen kan ved forskrift fastsette at § 14 om konsesjonsplikt skal gjelde også for andre foretak som driver personopplysningsvirksomhet.

I konsesjonen kan det settes vilkår om innsamling, lagring og bruk av opplysningene, samt om kontroll, om innsynsrett for den opplysningene gjelder og om rett til å kreve seg slettet av register.

KAPITTEL 6 Databehandlingsforetak

§ 22

Virksomhet som består i å bearbeide personopplysninger for andre ved elektroniske hjelpemidler, må ikke settes i gang før Kongen har gitt samtykke til det. § 14 annet ledd gjelder tilsvarende.

Første ledd gjelder ikke dersom bearbeidelsen utelukkende skjer for andre foretak innen samme konsern.

Kongen kan gi utfyllende forskrifter om hva som skal regnes som databehandlingsforetak ved anvendelse av første ledd, og kan ved forskrift eller enkeltvedtak gjøre unntak fra de enkelte bestemmelser i dette kapitlet.

§ 23

Foretak som må ha konsesjon etter § 22 første ledd, må ikke uten avtale med oppdragsgiveren anvende opplysningene til andre formål enn det oppdraget gjelder. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse.

§ 24

Foretaket skal treffe de sikringstiltak som trengs.

Kongen kan ved forskrift eller for det enkelte foretak gi bestemmelser om de sikringstiltak som skal gjennomføres.

KAPITTEL 7 Adresserings- og distribusjonsvirksomhet

§ 25

Virksomhet som består i å selge eller på annen måte tilby adresser

for grupper av personer, eller i å utføre oppdrag for utsending av reklame og andre meddelelser til slike grupper, kan ikke settes i gang før Kongen har gitt samtykke til det. § 14 annet ledd gjelder tilsvarende.

Kongen kan gi utfyllende forskrift om hvilke foretak som er konsesjonspliktige etter første ledd, og kan ved forskrift eller enkeltvedtak gjøre unntak fra de enkelte bestemmelser i kapitlet.

§ 26

Et register til bruk for virksomhet som er nevnt i § 25 første ledd, kan ikke inneholde

1) opplysninger om rase, eller politisk eller religiøs oppfatning
2) opplysninger om at en person har vært tiltalt eller dømt i straffesak
3) opplysninger om helseforhold eller misbruk av rusmidler
3) opplysninger om seksuelle forhold
5) andre opplysninger om familieforhold enn slike som gjelder slektskap eller familiestatus, formuesordningen mellom ektefeller og forsørgelsesbyrde

Kongen kan ved forskrift eller enkeltvedtak ytterligere begrense foretakets adgang til å registrere personopplysninger, og regulere bruken av registrerte opplysninger.

§ 27

Uten hinder av bestemmelsene i § 26 kan foretaket sende meldinger på grunnlag av kunde- og medlemsregistre som stilles til rådighet av oppdragsgiveren. Slike registre må bare nyttes til å sende meldinger om oppdragsgiverens varer eller tjenester o.l., og de kan ikke overlates til andre.

§ 28

Foretak skal i sine registre slette enhver som ber om det. En registrert kan kreve å få opplyst hvem som er foretakets kilde for registreringen.

Gjelder kravet om sletting slikt register som er nevnt i § 27, skal kravet sendes til oppdragsgiveren, som plikter å påse at vedkommende blir strøket som adressat ved seinere bruk av registeret. Den som har satt fram kravet, skal underrettes om videresendingen og om oppdragsgiverens navn.

§ 29

Kongen kan ved forskrift eller for det enkelte foretak gi bestemmelser med sikte på å hindre at personopplysninger blir brukt i strid med §§ 26 og 27 og for å sikre gjennomføringen av reglene i § 28.

§ 30

Kongen kan ved forskrift bestemme

1) at §§ 26 og 28 skal gjelde tilsvarende for foretak som i enkeltstående tilfeller påtar seg oppdrag som er nevnt i § 25 første ledd,
2) at visse typer opplysninger ikke skal kunne anvendes for utvalg av adressater ved utsending av meldinger for foretakets egne varer og tjenester o.l., samt at § 28 skal gjelde tilsvarende for slike adresselister.

KAPITTEL 8 Opinions- og markedsundersøkelser

§ 31

Virksomhet som består i å utføre opinions- eller markedsundersøkelser for andre, kan ikke sette i gang før Kongen har gitt samtykke til det. § 14 annet ledd gjelder tilsvarende.

Kongen kan gi utfyllende forskrift om hvilke foretak som er konsesjonspliktige etter første ledd, og kan ved forskrift eller enkeltvedtak gjøre unntak fra de enkelte bestemmelser i dette kapitlet.

§ 32

Personopplysninger som noen gir under opinions- eller markedsundersøkelser, må ikke meddeles videre i en slik form at opplysningen kan henføre til en enkelt person.

Opplysninger som er mottatt for opinions- og markedsundersøkelser, må ikke brukes for andre formål.

§ 33

Uten samtykke fra den opplysningene gjelder, må opplysning om navn, fødselsdato, fødselsnummer eller liknende ikke innføres i register som bearbeides ved elektroniske hjelpemidler. Heller ikke må slike opplysninger innføres i et annet register som er særskilt utformet med sikte på at opplysningene skal være lett tilgjengelige og anvendelige.

Uten samtykke fra den opplysningen gjelder, må innsamlete opplysninger ikke lagres i mer enn et halvt år i slik form at de kan henføres til en enkelt person.

§ 34

Kongen gir nærmere forskrifter om slik virksomhet som er nevnt i § 31. Forskriftene kan bl.a. inneholde bestemmelser om innhenting av opplysninger, om lagring av innhentede opplysninger, og andre bestemmelser som skal sikre at innsamlede personopplysninger ikke nyttes på urett måte eller kommer på urette hender.

§ 35

Kongen kan ved forskrift bestemme at §§ 32 til 34 skal gjelde også for foretak som i enkeltstående tilfelle påtar seg slike oppdrag som er nevnt i § 31 første ledd, og for foretak som setter i verk slike undersøkelser for sin egen administrasjon og virksomhet.

KAPITTEL 9 Overføring til utlandet, m.m.

§ 36

Register som omfattes av § 9 første ledd må ikke overføres til utlandet uten samtykke av Kongen.

Personopplysninger som er innsamlet her i riket, må ikke overføres til utlandet uten samtykke av Kongen når formålet er å innføre opplysningene i et register.

Kongen kan ved forskrift gjøre unntak fra første og annet ledd. Det kan fastsettes at disse bestemmelser ikke skal gjelde i forhold til enkelte andre land.

§ 37

Kongen kan gi forskrift om samarbeid mellom Datatilsynet og tilsynsmyndigheter i andre land. I slik forskrift kan det fastsettes etter § 11, § 14, § 22, § 25, § 31 eller § 36.

KAPITTEL 10 Straff og erstatning

§ 38

Med bøter eller fengsel inntil ett år eller begge deler straffes den som forsettlig eller aktløst

1) unnlater å innhente samtykke etter § 9, § 13 tredje ledd, § 14, § 22, § 25, § 31 eller § 36
2) overtrer regler eller vilkår fastsatt etter § 11, § 14, § 22, § 25, § 31 eller § 36,
3) bruker opplysninger i strid med reglene i § 16, § 18, § 23, § 26, § 27, § 32 eller § 33
4) unnlater å etterkomme krav fra Datatilsynet etter § 5 eller § 8
5) unnlater å etterkomme krav om opplysninger etter § 7 eller § 20 eller krav om sletting etter § 28
6) unnlater å gi melding etter § 19 til den opplysningene gjelder.

Medvirkning straffes på samme måte. I forskrift som gis i medhold av loven, kan det fastsettes at overtreding av forskriften skal straffes med bøter eller fengsel inntil ett år eller begge deler.

§ 39

Er en overtreding som nevnt i § 38 begått av noen som har handlet på vegne av et foretak, kan bøtestraff idømmes foretaket, selv om ingen kan straffes etter § 38.

Ved utmåling av straff etter denne paragrafen skal det særlig legges vekt på om overtredingen er foretatt for å fremme foretakets interesser, og om overtredingen er foretatt for å fremme foretakets interesser, og om foretaket har hatt fordel av overtredingen.

Straffelovens § 28 gjelder ikke bøtestraff etter denne paragraf.

§ 40

Har foretak som driver virksomhet som nevnt i § 13, meddelt opplysninger i strid med bestemmelser gitt i eller i medhold av loven her, eller meddelt opplysninger som viser seg uriktige eller åpenbart misvisende, skal foretaket erstatte det tap som påføres den opplysningene gjelder. Dette gjelder uten hensyn til om det er utvist skyld fra noen som har opptrådt på vegne av eller i tjeneste hos foretaket.

KAPITTEL 11 Forholdet til andre lover. Ikraftsetting

§ 41

Konsesjonsplikten etter § 9 jfr. § 10 gjelder ikke for personregistre i organ for stat eller kommune som er opprettet ved egen lov. Også for slike registre skal det likevel fastsettes regler som nevnt i § 11, i den utstrekning det ikke er fastsatt noe annet i eller i medhold av heimelsloven. Også de andre bestemmelsene i loven gjelder for slike registre i den utstrekning det ikke er fastsatt noe annet i eller i medhold av heimelsloven.

§ 42

Loven trer i kraft den dag Kongen bestemmer.

For personregistre som er opprettet før loven trer i kraft, og som omfattes av § 9, skal det søkes om samtykke innen en frist som Kongen fastsetter. Forutsatt at søknad er kommet inn innen fristen, kan personregisteret brukes uendret inntil det er fastsatt regler etter § 11. Reglene i annet ledd gjelder tilsvarende når det kreves samtykke etter kapitlene 5-9.

§ 43

Fra loven trer i kraft gjøres følgende endringer i andre lover.

1. Lov 24.mai 1961 nr. 1 om sparebanker
   § 21 nytt annet ledd skal lyde:
   Denne bestemmelse er likevel ikke til hinder for at banken driver kredittopplysningsvirksomhet i samsvar med lovgivningen for slik virksomhet.

2. Lov 24 mai 1961 nr 2 om forretningsbanker
   § 18 nytt annet ledd skal lyde:
   Denne bestemmelse er likevel ikke til hinder for at banken driver kredittopplysningsvirksomhet i samsvar med lovgivningen for slik virksomhet.

3. Lov 11 juni 1976 nr 71 om finansieringsvirksomhet
   § 15 nytt annet ledd skal lyde:
   Denne bestemmelse er likevel ikke til hinder for at foretaket driver kredittopplysningsvirksomhet i samsvar med lovgivningen for slik virksomhet.

VEDLEGG 2: Kongelig resolusjon av 21. desember 1979

I. Delegering av Kongens myndighet i medhold av personregisterloven.
II. Bestemmelser om unntak fra personregisterloven i medhold av lovens § 1 fjerde ledd.
III. Bestemmelser om unntak etter lovens §§ 4, 5 og 7
IV. Ikraftsettelse av personregisterloven, jfr. lovens § 42.

I

Lov om personregistre m.m. av 9.juni 1978 inneholder en rekke bestemmelser der myndighet er gitt til Kongen. Det var forutsetningen at en rekke av Kongens fullmakter måtte delegeres i forbindelse med ikraftsettelse av loven.

Lovens § 9 inneholder en regel om konsesjonsplikt for opprettelse av personregistre. Det har vært vurdert å delegere Kongens myndighet til å gi konsesjon. De aktuelle muligheter vil etter Justisdepartementets oppfatning være at myndigheten delegeres til Justisdepartementet som Datatilsynet administrativt sorterer under, til det fagdeparetement som virksomheten (personregisteret) hører under eller til Datatilsynet. Justiskomiteen uttalte i forbindelse med behandlingen av loven (Innst. O. nr. 47 for 1977-78 s. 7):

> "Spørsmålet om hvem som skal utøve konsesjonsmyndighet er drøftet i proposisjonen, men ikke avklart. Komiteen mener det er naturlig at konsesjonsmyndigheten delegeres til Datatilsynet både for private og offentlige registre med Justisdepartementet som klageinstans. Som et frittstående organ med personregistre og personvern som arbeidsfelt vil Datatilsynet være godt egnet til å treffe disse avgjørelser. Også hensynet til en likest mulig behandling av de ymse registertyper taler for en slik ordning".

Justisdepartementet har ikke funnet grunn til en annen løsning enn det som følger av denne uttalelse. En har likevel funnet at det må gjøres to spesielle unntak. Det ene gjelder de registre Datatilsynet selv måtte opprette. Når det gjelder konsesjonsbehandlingen av disse, foreslår en at konsesjonsmyndigheten legges til Justisdepartementet med Kongen som klageinstans. Når det gjelder Justisdepartementets egne registre og registre i organer underlagt Justisdepartementet, foreslås konsesjonsmyndigheten lagt til Datatilsynet med Kongen som klageinstans.

Justisdepartementet har videre funnet det hensiktsmessig å delegere til Datatilsynet Kongens myndighet til å gi konsesjon for visse typer av virksomhet, jfr. lovens § 14 første ledd, § 22 første ledd, § 25 første ledd og § 31 første ledd.

Lovens § 16 inneholder regler om hvilke opplysninger som ikke kan brukes som ledd i kredittopplysningsvirksomhet. Etter § 16 annet ledd kan Kongen likevel gi samtykke til at opplysninger som nevnt i paragrafens første ledd kan samles inn og meddeles videre. Myndighet til å gi slikt samtykke foreslås delegert til Datatilsynet.

Etter lovens § 36 kreves det samtykke fra Kongen dersom en vil overføre et register som omfattes av konsesjonsplikten etter lovens § 9 til utlandet. På samme måte kreves det samtykke fra Kongen dersom personopplysninger som er samlet inn her i riket skal overføres til utlandet når formålet er å innføre et register som ville være konsesjonspliktig etter lovens § 9. Også myndighet til å gi slikt samtykke foreslås delegert til Datatilsynet.

For øvrig foreslås Kongens myndighet delegert til Justisdepartementet med enkelte unntak. Kongens myndighet etter lovens § 1 fjerde ledd til å unnta enkelte typer av registre fra personregisterloven foreslås ikke delegert. Kongens myndighet etter lovens § 2 foreslås heller ikke delegert. Etter lovens § 3 kan Kongen gi Datatilsynet ytterligere oppgaver ut over det som fremgår av loven som gjelder bruk m.m. av personregistre eller bruk av personopplysninger ellers. Kongens myndighet på dette punkt foreslås ikke delegert.

Det er Justisdepartementets forutsetning at det bør skje en viss delegering fra Justisdepartementet til Datatilsynet. Dette forutsettes gjort i de forskrifter Justisdepartementet vil gi i medhold av den her foreslåtte delegerte myndighet. En forutsetter at adgangen etter loven til å treffe enkeltvedtak i stor utstrekning delegeres til Datatilsynet og med Justisdepartementet som klageinstans.

II

Etter personregisterlovens § 1 fjerde ledd kan Kongen bestemme at loven ikke skal gjelde for visse typer personregistre . I forbindelse med denne bestemmelse uttalte justiskomiteen (Innst. O. nr. 47 for 1977-78 s. 4):

> "Komiteen har merket seg departementets vurdering av unntak fra loven i sin helhet. Det synes rimelig - og uten skade for lovens formål - at vanlige foreningers medlemskartotek som er ført manuelt, unntas fra loven med en gang. Med vanlige foreninger tenkes det her på lokale foreninger innenfor avholds- og idrettsbevegelsen, religiøse foreninger, hobbyklubber o.l. Politiske partier, fagbevegelsens og yrkesorganisasjonenes lokale avdelinger og lag kommer også inn i denne sammenheng. Komiteen er av den oppfatning at loven i utgangspunktet bør favne vidt fordi den regulerer et nytt og vanskelig område. Men vi bør samtidig søke å unngå en detaljregulering av uvesentlige forhold".

Justisdepartementet har ikke funnet det nødvendig å unnta fra loven registre av den typen som er nevnt. Det finnes dog en type av registre som etter lovens § 1 vil være et personregister, men som er av en karakter som gjør at det etter Justisdepartementets

oppfatning er hensiktsmessig med et unntak. En tenker på offentlige publikasjoner og bøker som pr. definisjon vil være et personregister og inngå under loven. På denne bakgrunn foreslår Justisdepartementet at en i medhold av lovens § 1 fjerde ledd unntar bøker, tidsskrifter e.l. som etter personregisterlovens § 1 er et personregister eller inneholder et personregister, dog slik at lovens bestemmelser gjelder for utarbeidelsen og utgivelsen av slike personregistre som ikke er publisert før lovens ikrafttredelsestidspunkt.

Et spesielt forhold har vært vurdert i forbindelse med unntak fra loven. Det gjelder personregistre av sikkerhetsmessig og beredskapsmessig betydning. Behovet for unntak for slike registre skyldes at dersom lovens bestemmelser gjøres gjeldende for disse registre, vil flere personer få kunnskap om innholdet i registrene, noe som vil innebære større fare for at opplysningene kan bli kjent. De registre som her er aktuelle er personregistre som føres av Overvåkingspolitiet samt personregistre i Forsvaret.

Justisdepartementet er likevel av den oppfatning at disse registrene også bør omfattes av loven. Det er dog etter Justisdepartementets oppfatning klart at det for enkelte registre eller for enkelte opplysninger i slike registre må gjøres spesielle unntak fra lovens bestemmelser, f.eks. unntak fra innsynsretten, unntak fra oppføring i fortegnelsen etter § 4 og unntak etter § 5. Det vises til avsnitt III nedenfor.

III

Selv om personregistre som er nødvendige ut fra beredskapsmessige hensyn eller hensynet til rikets sikkerhet ikke unntas fra lovens områder, jfr. avsnitt II foran, er det av de nevnte grunner behov for særskilte unntak fra enkelte av bestemmelsene i loven. Dette gjelder unntak fra oppføring i fortegnelsen etter § 4 , unntak fra retten til å kunne kreve opplysninger etter § 5 og unntak fra retten til å kreve innsyn i registrene etter § 7.

På denne bakgrunn foreslår Justisdepartementet at registre som er opprettet av hensyn til rikets sikkerhet eller av beredskapshensyn unntas fra lovens §§ 4 , 5 og 7. Det foreslås at uenighet mellom den registeransvarlige og Datatilsynet om et register går inn under denne bestemmelse, avgjøres av Justisdepartementet, som også kan bestemme i hvilken utstrekning unntaket skal gjelde for det enkelte register.

Registre av den karakter som er nevnt, må undergis konsesjonsbehandling av Datatilsynet. Det forutsettes imidlertid at det under konsesjonsbehandlingen ikke gis opplysninger som er unntatt etter de foran nevnte bestemmesler med mindre Kongen samtykker.

IV

Etter personregisterlovens § 42 første ledd skal loven settes i kraft fra den dag Kongen bestemmer. Justisdepartementet foreslår at loven settes i kraft 1.januar 1980.

Det vil i en del tilfeller være aktuelt med unntak fra innsynsretten etter lovens § 7 for det enkelte register.

Oversikten over hvilke registre dette gjelder og hvilke unntak som må gjøres, vil en først få i forbindelse med behandlingen av det enkelte personregister.

Dette vil enten være tilfelle i forbindelse med en konsesjonsbehandling , eller i forbindelse med en særlig søknad om unntak fra innsynsretten etter lovens § 7. Innsynsretten kan ikke gjøres gjeldende fullt ut fra 1.januar 1980 uten at spesielle unntak har vært vurdert. En har ikke funnet det mulig å oppstille generelle unntaksregler som ivaretar de aktuelle interesser fullt ut. På denne bakgrunn finner departementet at ikraftsettelse av lovens § 7 først bør skje fra 1.juli 1980, dog slik at søknad om unntak fra innsynsretten kommet inn før 1.juli 1980 gis oppsettende virkning.

For personregistre som er opprettet før loven trer i kraft og som omfattes av lovens § 9, skal det søkes om samtykke innen en frist som Kongen fastsetter. Justisdepartementet finner det rimelig å foreslå at fristen settes til 31.desember 1980.

JUSTISDEPARTEMENTET TILRÅR

I. Kongens myndighet etter personregisterlovens § 4 tredje ledd, § 5 tredje ledd, § 7 fjerde ledd, § 7 femte ledd, § 9 annet ledd, § 9 fjerde ledd, § 13 annet ledd, § 17 annet ledd, § 21 første punktum, § 22 tredje ledd, § 24 annet ledd, § 26 annet ledd,§ 29, § 30, § 31 annet ledd, § 34, § 35, § 36 tredje ledd og § 37 delegeres til Justisdepartementet.

   Kongens myndighet etter personregisterlovens § 9 første ledd delegeres til Datatilsynet med Justisdepartementet som klageinstans. I de tilfeller der Datatilsynet er konsesjonssøker, skal søknaden avgjøres av Justisdepartementet. I de tilfeller der Justisdepartementet er konsesjonssøker, er Kongen klageorgan. Kongens myndighet etter personregisterlovens § 13 tredje ledd, § 14 første ledd, § 16 annet ledd, § 22 første ledd, § 25 første ledd, § 31 første ledd og § 36 første og annet ledd delegeres til Datatilsynet med Justisdepartementet som klageinstans.

II. Følgende registertyper unntas fra personregisterloven i medhold av lovens § 1 fjerde ledd :
   1) Bøker, tidsskrifter e.l. som etter personregisterlovens § 1 er personregistre eller inneholder personregistre. Lovens bestemmelser gjelder likevel for utarbeidelsen og utgivelsen av slike personregistre som ikke er publisert før lovens ikrafttredelse.

III. Personregistre som er nødvendige ut fra beredskapshensyn eller hensynet til rikets sikkerhet, unntas fra personregisterloven §§ 4,5 og 7. Uenighet mellom den registeransvarlige og

Datatilsynet om et register går inn under denne bestemmelse avgjøres av Justisdepartementet, som også kan bestemme i hvilken utstrekning unntaket skal gjelde for det enkelte register.

IV. Lov om personregistre m.m. trer i kraft fra 1.januar 1980 med unntak av lovens § 7 som trer i kraft fra 1.juli 1980. Søknad om unntak fra lovens § 7 som er kommet inn til Datatilsynet før 10. juli 1980 gis oppsettende virkning.

Søknad som nevnt i personregisterlovens § 42 annet og tredje ledd må sendes inn innen 31.desember 1980.

Ad. ref. nr. 86
Resolusjon av 21.desember 1979
Avgjort av Kongen

VEDLEGG 3: Forskrifter i medhold av lov av 9. Juni 1978 NR. 48 om personregistre m.m.

Gitt av Justisdepartementet 21. desember 1979
med endringer av 10. mars 1981,
jfr. kgl. resolusjon 21. desember 1979.

KAP. 1. OM INNSYNSRETTEN.

(Personregisterloven § 7 fjerde og femte ledd.)

§ 1-1

Svar på henvendelser som nevnt i personregisterloven § 7 første ledd skal gis snarest mulig og senest innen en måned.

Svaret skal gis skriftlig dersom ikke den som benytter innsynsretten samtykker i at svaret gis muntlig eller på annen måte.

§ 1-2

Svar på henvendelser som nevnt i personregisterloven § 7 annet ledd skal gis snarest mulig og senest innen en måned. Dersom innsynsretten kan motvirke mulihetene for å få en sak som er under behandling avklart, kan institusjonen fastsette at vedkommende ikke skal ha adgang til opplysningene så lenge undersøkelser pågår, (jfr. forvaltningsloven § 20 første ledd).

Den registeransvalige bestemmer ellers, ut fra hensynet til forsvarlig saksbehandling, hvordan dokumentene eller opplysningene skal gjøres tilgjengelig for vedkommende. På anmmodning skal vedkommende gis skriftlig svar ved utskrift eller avskrift fra registeret.

§ 1-3

Svar på henvendelser som nevnt i personregisterloven § 7 tredje ledd skal gis umiddelbart.

Svaret skal gis skriftelig dersom ikke den som benytter innsynsretten samtykker i at svaret gis muntlig eller på annen måte.

§ 1-4

Datatilsynet gis myndighet som nevnt i personregisterloven § 7 femte ledd til ved enkeltvedtak å fastsette unntak fra innsynsretten. Datatilsynet kan også ved enkeltvedtak fastsette nærmere regler eller vilkår for bruk av retten, herunder unntak fra reglene i dette kapittel.

§ 1-5

Innsynsrett etter lovens § 7 annet ledd i opplysninger som ikke lagres eller bearbeides ved elektroniske hjelpemidler, skal også gjelde for de registre over nåværende eller tidligere ansatte, personale eller representanter som finnes i privat næringsvirksomhet, foreninger eller stiftelser, jfr. lovens § 7 fjerde ledd.

Som interne dokumenter som etter § 7 annet ledd kan unntas fra innsyn, skal i denne sammenheng regnes alle dokumenter arbeidsgiver selv utarbeider for sin interne saksforberedelse samt dokumenter som er utarbeidet for den interne saksforberedelse av særskilte rådgivere eller sakkyndige, eller av annen sammenslutning eller stiftelse innenfor eget konsern eller organisasjon.

Også dokumenter om å innhente dokumenter nevnt i denne bestemmelse kan unntas fra innsyn.

Selv om dokumentet er unntatt fra annet og tredje ledd bør vedkommende ha rett til å gjøre seg kjent med de deler av dokumentet som inneholder faktiske opplysninger eller sammendrag eller annen bearbeidelse av faktum. Dette gjelder likevel ikke faktiske opplysninger som finnes i annet dokument som vedkommende har innsyn i.

KAP. 2. FRITAK FRA KONSESJONSPLIKT.

(Personregisterloven § 9 annet ledd.)

§ 2-1

Personregistre som omfattes av dette kapittel er unntatt fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Vilkårene for konsesjonsfrihet er at kravene til registrenes innhold m.v. i §§ 2-2 til og med 2-15 følges, og at følgende regler overholdes:

(1) FORMÅL
Registeret må ikke brukes til andre formål enn det som følger av typebetegnelsene i §§ 2-2 til og med 2-15, eller i strid med andre lovregler som gjelder for føringen eller bruken av registeret.

(2) UTLEVERING
Personopplysninger må ikke utleveres fra registeret til utenforstående, unntatt når utlevering skjer
a) med samtykke fra den opplysningene gjelder,
b) til annen sammenslutning eller stiftelse innenfor eget konsern (jfr. lov av 4. juni 1976 nr. 59 om aksjeselskaper § 2-1).
c) med hjemmel i lov, eller i forskrift gitt med hjemmel i lov,
d) med hjemmel i avtale mellom partene i arbeidslivet,
e) som ledd i betalingsinnkreving (inkasso),
f) fra registre som nevnt i §§ 2-2 og 2-12 som

nødvendig ledd i opprettelse og administrasjon av kollektive forsikringsordninger,

g) for registre som nevnt i § 2-12 til registre for utarbeidelse av lønnsstatistikk som har konsesjon etter personregisterloven § 9. Denne bestemmelse er ikke til hinder for at annet kan bestemmes i avtale mellom partene i arbeidslivet,

h) fra registre som nevnt i § 2-4 til annen bank, etter beslutning fra styret eller noen som har fullmakt fra styret til å avgjøre spørsmål om utlevering,

i) fra registre som nevnt i § 2-5 til andre livsforsikringsselskaper eller deres bransjeorganisasjoner, etter beslutning fra styret eller noen som har fullmakt til å avgjøre spørsmål om slik utlevering.

Oppbevaring eller behandling av personopplysninger hos et databehandlingsforetak som har konsesjon etter ^prl; § 22, eller hos et adresserings- eller distribusjonsforetak som har konsesjon etter loven § 25, regnes ikke som utlevering når dette skjer etter oppdrag fra registerets eier.

Denne bestemmelse om utlevering gjelder ikke for personregistre som nevnt i §§ 2-11, 2-13 og 2-15.

(3) KOPLING.
Registeret må ikke koples sammen med andre personregistre, unntatt når koplingen

a) skjer med hjemmel i lov,

b) har hjemmel i avtale mellom partene i arbeidslivet,

c) er ledd i utveksling og sammenholding av opplysninger i et foretaks vanlige administrative rutiner,

d) går ut på å sammenligne navn og adresser for å unngå dobbeltforsendelser o.l.,

e) skjer i forbindelse med utlevering som nevnt i punkt (2) bokstav f.

Registre som nevnt i § 2-4 og § 2-8 regnes i denne sammenheng som ett register.

(4) SIKRING.
Den registeransvarlig må sørge for forsvarlig sikring av de registrerte personopplysninger, slik at ikke noen får tilgang til opplysningene uten å ha rett til eller krav på dem.

Datatilsynet kan gi pålegg som ansees som nødvendige for å oppnå forsvarlig sikring.

Fødselsnummer må ikke benyttes utenpå postsendinger. For organ i staten vises for øvrig til gjeldende sikkerhets- og databeskyttelsesinstruks med utfyllende bestemmelser (datasikkerhetsdirektivet). Denne bestemmelse gjelder ikke for registre som nevnt i § 2-15.

(5) SLETTING.
Tidligere medlemmer, kunder, abonnenter og leverandører skal slettes fra registre som nevnt i §§ 2-2, 2-3, 2-4, 2-5 og 2-6 når vedkommende krever det og andre lovregler ikke er til hinder for sletting.

Utsendelsene som registre som nevnt i § 2-7 brukes til, må påføres avsenders navn og adresse. Enhver som ber om det kan kreve seg slettet fra registeret.

Opplysning om "lånenummer" i utlånsregister som nevnt i § 2-8 skal biblioteket slette av eget tiltak når den utlånte bok er tilbakelevert.

§ 2-2

Foreningers medlemsregistre unntas fra konssjonsplikten etter personregisterloven § 9 første ledd.

Med et slikt register menes en fortegnelse over en forenings nåværende og tidligere medlemmer som ikke inneholder andre personopplysninger enn:

(1) navn
(2) adresseopplysninger
(3) opplysninger om nummer (anropsnummer) for telefon, teleks og andre teletjenester
(4) medlemsnummer
(5) medlemskoder (opplysninger om type medlemsskap o.l.)
(6) tillitsverv
(7) kjønn
(8) fødselsdato
(9) data for distribusjon av trykksaker, publikasjoner o.l.
(10) opplysninsger om kurs, utdannelse o.l. innen foreninger eller i tilknytning til denne
(11) utdannelse, stilling, arbeidsgiver
(12) kontingentopplysninger
(13) utlånte eiendeler
(14) lønnsopplysninger
(15) resultater fra idrettskonkurranser o.l.

§ 2-3

Kunde-, abonnent- og leverandørregistre unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Med et slikt register menes register over kunder/abonnenter og/eller leverandører som ikke inneholder andre personopplysninger enn :

(1) navn
(2) kontaktnummer og kontaktperson
(3) konsernopplysninger
(4) adresseopplysninger
(5) opplysninger om nummer (anropsnummer) for telefon, teleks og andre teletjenester
(6) kontonummer bank/post og andre opplysninger i den

sammenheng
(7) rubriseringsdata (så som kategori kunde/leverandør, distrikt, type varer, kontonummer i regnskap, kunde-/leverandørnummer, andre opplysninger til bruk i statistikk og annen bedriftsintern avregning og andre opplysninger som ikke angår fysiske personer eller personlige forhold)
(8) inkasso- og utbetalingsopplysninger
(9) saldoinformasjon
(10) kredittgrense
(11) betalingsbetingelser
(12) aldersfordeling av saldoposter
(13) purringsstatus

§ 2-4

Kunderegistre i banker som omfattes av :

- lov av 23. april 1892 om Norges Bank
- lov av 1. mars 1946 nr. 3 om Den Norske Stats Husbank
- lov av 10. desember 1948 nr. 2 om Norges Postsparebank
- lov av 15. juni 1949 nr. 1 om Norges Kommunalbank
- lov av 24. mai 1961 nr. 1 om sparebanker
- lov av 24. mai 1961 nr. 2 om forretningsbanker
- lov av 5. februar 1965 nr. 2 om Statens landbruksbank
- lov av 28. april 1972 nr. 22 om Statens Fiskarbank
- lov av 25. mars 1977 nr. 14 om Den Norske Industribank A/S

unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Kunderegistre som er unntatt fra konsesjonsplikten etter første ledd kan bare benyttes i forbindelse med innlån, utlån, betalingsformidling, inkasso, forvaltning og andre ordinære banktjenester.

I det enkelte kunderegister kan følgende personopplys- ninger registreres:

(1) Kundeopplysninger
Med kundeopplysninger menes personopplysninger om bankens kunder, kausjonister, og andre som banken har saklig behov for å registrere opplysninger om på grunn av deres forhold til kunden (jfr. personregisterloven § 6 første ledd).

Følgende kundeopplysninger kan registreres :
a) navneopplysninger
b) adresseopplysninger (bosteds- , arbeids-, adviserings- og tilskriveradresser)
c) opplysninger om anropsnummer for telefon, teleks og andre teletjenester
d) fødselsnummer
e) foretaksnummer og arbeidsgivernummer
f) kjønn
g) antall konti (egne, kausjonist, garantist o.l.)
h) sivilstand
i) stillingsbetegnelse
j) notatfelt med rent administrative opplysninger

om kundeforholdet (disposisjonsforhold, sperringer o.l.) Personopplysninger som nevnt i personregisterloven § 6 annet ledd tillates ikke registrert i notatfelt

k) kundetype og kundekode
l) formues- og inntektsforhold, og beløpsangivelse for beregnet kredittverdighet
m) kundeopplysninger (opprettelse, avslutning o.l.)
n) henvisninger til andre som banken har saklig behov for å registrere på grunn av deres forhold til kunden (kausjonister, garantister, konsern, datterselskap, arbeidsgiver e.l.)

(2) Konto- og oppdragsopplysninger.
Med konto- og oppdragsopplysninger menes opplysninger om de enkelte konti eller oppdrag.

Følgende konto- og oppdragsopplysninger kan registreres :

a) kontonummer og oppdragsnummer
b) andre numre i tilknytning til kontoen (depotnummer, disponentnummer, bankkortnummer, kausjonistnummer, betalingskortnummer, aksjenummer m.v.)
c) åpnings-, endrings-, avslutningsdato, og andre dato opplysninger vedrørende kontoen eller oppdraget
d) rente-, dekort-, provisjonsbetingelser og gebyrer
e) saldi, gebyrbeløp, rentebeløp debet/kredit, omkostninger, provisjoner agio, og andre statusopplysninger
f) avdrags-, termin-, og forfallsopplysninger
g) opplysninger om purringer, overtrekk og inkasso
h) disposisjonsopplysninger, stikkord
i) innvilgede lån
j) opplysninger om stillet sikkerhet (prioritet, takst, utløpsdatoer o.l.)
k) henvisningsopplysninger av betydning for disponeringen av kontoen eller oppdraget
l) notatfelt med rene administrative opplysninger om kontoen eller oppdraget (disposisjonsforhold, sperringer o.l.). Personopplysninger som nevnt i personregisterloven § 6 annet ledd tillates ikke registrert i notatfeltet
m) kontoanalysedata
n) betalingsmottakers/kreditorers kontonummer, navn adresse og fødselsnummer
o) opplysninger som er nødvendige for å hindre uttak på sperret konto

(3) Transaksjonsopplysninger.
Med transaksjonsopplysninger menes opplysninger som registreres i forbindelse med bruk av kontoen, inklusive transaksjoner som tilføres automatisk slik som renter, provisjoner o.l.

Følgende transaksjonsopplysninger kan registreres:

a) transaksjonsbeløp og valutasort

b) arkivreferanse og terminalidentifikasjon
c) ID-nummer (ikke fødselsnummer), bilagsnummer, sjekknummer o.l.
d) tekstkode, tekst og annen beløpsidentifikasjon
e) bokføringsdato, valuteringsdato, og andre tidsbestemmelser av transaksjonsforløpet
f) henvisninger til motpost
g) førings- og behandlingskoder

(4) Administrative opplysninger og interne referanser. I tilknytning til opplysninger som nevnt i punkt (1) til og med punkt (3) ovenfor, kan det registreres administrative opplysninger som systemet må benytte för at det skal kunne arbeide i samsvar med de kunde-, konto-, oppdrags-, og transaksjonsopplysninger som er nevnt. Dessuten kan det registreres interne referanser som bare benyttes for å vise til andre rutiner eller registre, og som eller ikke har behandlingsmessige konsekvenser.

(5) Statistikk.

Felter for klassifikasjon og koding av opplysninger til å utarbeide offentlig og intern statistikk kan benyttes for personopplysninger som tillates registrert etter punkt (1) til og med punkt (3) ovenfor. Statistikk må ikke utarbeides i en slik form at opplysningene direkte eller indirekte kan føres tilbake til den enkelte konto eller kunde.

§ 2-5

Forsikrings- og utlånsregistre i livsforsikringsselskaper som omfattes av lov av 19.juni 1911 nr. 1 om forsikringsselskaper kap. 3, unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Med et forsikringsregister menes et personregister over forsikringstakere og andre som er tilknyttet forsikringspoliser som er tegnet i selskapet.

Livsforsikringsselskapenes forsikringsregister kan brukes til :

(1) den ordinære administrasjon av selskapets livs- og pensjonsforsikringer
(2) å beregne provisjon til salgsmedarbeidere og honorar til leger vedrørende utskriving av dødsattester, legeerklæringer o.l.
(3) å fremstille statistikk over premier, erstatningsytelser, kunder o.l. for revisjonsformål og for å kunne drive produktutvikling
(4) å fremstille grunnlagsdata for selskapets interne økonomiske og administrative rutiner
(5) å utarbeide tilbud om forsikringsdekning
(6) å gjennomføre oppfølgning av erstatningstilfeller og foreta risikobedømmelse ved bl.a. å gi opplysninger til bransjens felles organer (Nemnden for helsebedømmelse, og Livsforsikringsselskapenes registreringskontor
(7) å gjennomføre forsikringstekniske beregninger

(8) å kunne foreta informasjonsutveksling mellom organisasjoners medlemsregistre og for de personer som omfattes av forsikringen
(9) å gi kunder informasjon om selskapet og dets produkter.

Livsforsikringsselskapenes forsikringsregistre må ikke inneholde andre opplysninger enn :

(1) Personlige opplysninger om personer som er tilknyttet en forsikringspolise, herunder:
   a) navn og adresse
   b) fødselsnummer
   c) firmanummer
   d) kjønn
   e) sivilstand
   f) yrke
   g) polisenummer og medlemsnummer
   h) arbeidsgiver og organisasjon
   i) andre identifikasjonsopplysninger for de registrerte

(2) opplysninger om forsikredes helse, sykdomstilfeller og skader, herunder
   a) opplysninger om sykdommens eller skadens art og varighet
   b) dødsårsak

(3) Opplysninger om forsikringens verdi, dvs. opplysninger om
   a) selskapets forsikringsforpliktelser
   b) forsikringens aktuelle kapitalverdi
   c) data som inngår i beregning av disse

(4) Opplysninger om premiene, dvs. opplysninger om
   a) polisens premie
   b) betalingsbetingelser og betalingsforhold
   c) fradrag og tillegg i premien
   d) data som inngår i beregningen av disse
   e) data for styring av skattefradrag

(5) Opplysninger for gjennomføring av oppgjørs- og erstatningsberegninger, dvs.
   a) data for beregning av erstatningsbeløp, herunder forsikringsform, bonus m.v.
   b) trekk- og skatteopplysninger
   c) opplysninger om erstatningsmottaker

(6) Andre forsikringsopplysninger m.v.
   a) statistiske data
   b) forsikringstekniske data, herunder opplysninger og beregningsgrunnlag, nettopremier og opplysninger om indeksregulering
   c) provisjonsdata
   d) reassuransedata
   e) poliselånsdata
   f) styrings- og hjelpedata for EDB

Med et utlånsregister menes et personregister over enkeltpersoner og andre som er registrert i forbindelse med utlån.

Livsforsikringsselskapenes utlånsregistre kan brukes til selskapets ordinære administrasjon av sin utlånsvirksomhet.

Utlånsregistrene må ikke inneholde andre opplysninger enn:

(1) Opplysninger om personer og andre som er registrert i forbindelse med utlån, herunder
   a) navn og adresse
   b) fødselsnummer
   c) firmanummer
   d) lånenummer
   e) andre identifikasjonsopplysninger om de registrerte

(2) Opplysninger om lånet, herunder
   a) innvilget beløp, restlån, status og type
   b) rentesats, avdrag, antall terminer, og forfall
   c) lånets formål og oppsigelsesbestemmelser
   d) betalte renter og avdrag samt restanser

(3) Opplysninger om hva slags pant som er stillet i sikkerhet for lånet, herunder
   a) pantets betegnelse med eventuelt grunnboksnummer og bruksnummer
   b) pantets takstbeløp
   c) pantets type
   d) grunnkode og festetid

(4) Diverse opplysninger av statistisk, geografisk og intern art for klassifisering av lånet herunder
   a) tinglysningsopplysninger
   b) debitortype
   c) geografisk beliggenhet
   d) garantier
   e) båndlagte beløp
   f) prioriteter og beløp

§ 2-6

Leietakerregistre unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Med et slikt register menes et register over register- eierens leieboere som ikke inneholder andre personopplysninger enn:

(1) navneopplysninger
(2) adresseopplysninger
(3) fødselsnummer (såfremt registeret brukes til fordeling av ligningsmessig underskudd i borettslag)
(4) medlemsnummer i borettslag
(5) ansiennitetsopplysninger til bruk ved tildeling av leilighet
(6) medlemskontingentbeløp
(7) leilighetsnummer og adresse
(8) leilighetstype og størrelse
(9) leilighetens alder
(10) leilighetens verdi (takst) ved omsetning
(11) leilighetens omsetningsform
(12) leiebeløp fordelt på art (husleie, garasje, fyring

etc.)
(13) medlemmets tilknytning til leilighet (eier, fremleier, leier etc.)
(14) dato for innflytning
(15) betaling/restansedata for kontingentinnkreving
(16) betaling/restansedata for leieinnkreving
(17) oversikt over tidligere leietakere til bruk ved fordeling av ligningsmessig underskudd i borettslag
(18) bankkontonummer for automatisk belastning av leie på konto
(19) andre rent administrative opplysninger.

§ 2-7

Registre for utsendelse av publikasjoner/trykksaker som bare inneholder følgende personopplysninger unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd:

(1) navneopplysninger
(2) adresseopplysninger
(3) nummer (anropsnummer) for telefon, teleks og andre teletjenester
(4) yrke/tittel
(5) opplysninger nødvendige for utsendelse, unntatt opplysninger nevnt i personregisterloven § 6 annet ledd.

§ 2-8

Katalog-, låner- og utlånsregister i bibliotekene unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Med et katalogregister menes et register over et biblioteks titler som brukes som et hjelpemiddel i biblioteket og som kun inneholder følgende personopplysninger:

(1) signatur
(2) forfatter
(3) tittel
(4) utgavebetegnelse
(5) utgiversted og -år
(6) sidetall og antall bind
(7) tittelnummer

eller andre lignende opplysninger.

Med et låneregister menes en fortegnelse over samtlige lånere i biblioteket som ikke inneholder andre personopplysninger enn følgende:

(1) lånenummer
(2) navn
(3) alder
(4) adresseopplysninger
(5) yrke
(6) dato for utsendelse av lånekortet

Med et utlånsregister menes en fortegnelse over hvert enkelt av bibliotekets bøker e.l. som kun inneholder følgende personopplysninger:

(1) eksemplarnummer
(2) tilhørighet i bibliotek
(3) status
(4) utlånsdato
(5) forfallsdato
(6) lånenummer
(7) antall innkallinger sendt
(8) statistikk over antall utlån

§ 2-9

Advokaters arkiver/registre som ikke gjør bruk av elektroniske hjelpemidler unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Med et slikt register/arkiv menes en advokats fortegnelse over tidligere og nåværende klienter og motparter, samt andre med tilknytning til disse.

§ 2-10

Legers, tannlegers, psykologers eller annet godkjent helsepersonells registre som ikke gjør bruk av elektroniske hjelpemidler ut fra konsesjonsplikten etter personregisterloven § 9 første ledd.

§ 2-11

Registre opprettet i medhold av lov av 4. juni 1976 nr. 59 om aksjeselskaper § 3-8 unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd dersom det ikke inneholder slike opplysninger som nevnt i § 6 annet ledd.

§ 2-12

Register over den registeransvarliges nåværende eller tidligere ansatte, personale og representanter, unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd dersom

1. registeret ikke gjør bruk av elektroniske hjelpemidler
2. registeret gjør bruk av elektroniske hjelpemidler og ikke inneholder andre opplysninger enn:
   (1) navneopplysninger
   (2) adresseopplysninger
   (3) opplysninger om nummer (anropsnummer) for telefon, teleks og andre teletjenester
   (4) fødselsnummer og annet nummer knyttet til person (rullenummer/arbeidstakernummer)
   (5) rubriseringsdata, (såsom kategori, type ansatt/representant, distrikt, type varer, kontonummer i regnskap, representantkategori, andre opplysninger til bruk i statistikk og annen bedriftsintern avregning)
   (6) kjønn
   (7) nærmeste pårørende
   (8) sivilstand
   (9) stillingsbetegnelse
   (10) yrkesopplysninger som etter overenskomst eller

tariffavtale har betydning for lønns- og arbeidsvilkår
(11) opplysninger om utdannelse og praksis
(12) lønns- og provisjonsopplysninger
(13) bankkontonummer
(14) pensjonsopplysninger
(15) trekk- og skatteopplysninger
(16) ansettelses- og sluttdato (permisjoner e.l.)
(17) dødsdato
(18) fraværsdato, type fravær og varighet. Angivelse av sykdommens art tillates ikke registrert utover det som er pålagt ved lov av 4. februar 1977 nr. 4 § 20 om arbeidervern
(19) firmabil e.l.
(20) utlånte eiendeler
(21) lån til ansatte eller garanti for lån
(22) opplysning om den ansatte er mobiliserings-disponent (ja/nei) evt. militært løpenummer, grad, og rulleførende avdeling.

I tillegg til de opplysninger som er oppregnet ovenfor kan det i slike registre tas inn opplysninger når det er pålagt i medhold av gjeldende lover eller avtaler mellom partene i arbeidslivet.

§ 2-13

Forlagenes personarkiver/registre til bruk ved utgivelse av biografiske leksika, konversasjonsleksika og fagleksika unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

§ 2-14

Dags- og ukepressens personregister til bruk i journalistisk virksomhet unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

§ 2-15

Personregistre som kun inneholder personopplysninger om valgte eller oppnevnte representanter i organ opprettet i medhold av lov av 12. november 1954 nr. 1 om styret i kommunene, eller lov av 16. juni 1961 nr. 1 om fylkeskommuner, eller lov av 19. desember 1952 nr. 7 om Den norske kirkes ordning, unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Det samme gjelder personregistre som kun inneholder personopplysninger om Stortingets representanter eller medlemmer av Stortingerts kommiteer.

§ 2-16

Konsesjonsfrihet etter dette kapittel gjelder også når flere konsesjonsfrie registre føres som ett register. Forutsetningen for konsesjonsfrihet er dessuten at dette registeret ikke inneholder andre opplysninger enn det som er tillatt etter bestemmelsene for hver enkelt av de registrene som føres som ett. De øvrige vilkår for konse- sjonsfrihet for de enkelte registre må også overholdes.

KAPITTEL 3

FRITAK FRA KONSESJONSPLIKT MOT MELDEPLIKT

(Personregisterloven § 9 annet ledd)

Opphevet.

KAPITTEL 4

KONSESJON FOR KREDITT- OG PERSONOPPLYSNINGSVIRKSOMHET
(Personregisterloven § 13 annet ledd og § 17 annet ledd)

§ 4-1

Følgende virksomheter regnes ikke som kredittopplysnings-virksomhet:

(1) meldinger fra offentlige registre om rettigheter og heftelser i fast eiendom eller løsøre.
(2) meldinger fra banker (jfr. lov 23.april 1892 om Norges Bank, lov av 1. mars 1946 nr. 3 om Den Norske Stats Husbank, lov av 10. desember 1948 nr. 2 om Norges Postsparebank, lov av 15. juli 1949 nr. 1 om Norges Kommunalbank, lov av 24. mai 1961 nr. 1 om sparebanker, lov av 24. mai 1961 nr. 2 om forretningsbanker, lov av 5. februar 1965 nr. 2 om Statens Landbruksbank, lov av 28. april 1972 nr. 22 om Statens Fiskarbank og lov av 25. mars 1977 nr. 14 om Den Norske Industribank A/S) og fra finansieringsselskaper (jfr. lov av 4. juni 1976 nr. 71 om finansieringsvirksomhet) som gjelder dekningskontroll for sjekk eller annet uttak fra konto, diskontering av veksler og avbetalingskontrakter. Det samme gjelder når slike meldinger formidles for bank eller finansieringsselskap av et utenforstående foretak.
(3) meldinger til den opplysningene gjelder.
(4) utgivelse av ligningsdata.

§ 4-2

Følgende virksomheter unntas fra konsesjonsplikten etter personregisterloven § 14:

(1) banker, jfr. lov av 24. mai 1961 nr. 2 om forretningsbanker og lov av 24. mai 1961 nr. 1 om sparebanker.
(2) finansieringsvirksomhet i medhold av lov av 4. juni 1976 nr. 71 om finansieringsvirksomhet.
(3) statsbanker opprettet ved egen lov.

§ 4-3

Fødselsnummer må ikke benyttes utenpå postsendinger.

§ 4-4

Datatilsynet gis myndighet til ved enkeltvedtak å gjøre unntak som

nevnt i personregisterloven § 13 annet ledd annet punktum.

§ 4-5

Datatilsynet gis myndighet til ved enkeltvedtak å gi slike regler som nevnt i personregisterloven § 17 annet ledd.

KAPITTEL 5

KONSESJON FOR DATABEHANDLINGSFORETAK (Personregisterloven § 22 tredje ledd og § 24 annet ledd)

§ 5-1

Et forvaltningsorgan (jfr. forvaltningsloven § 1) som bare bearbeider personopplysninger for andre over-, under- eller sideordnede organer i samme etat, regnes ikke som databehandlingsforetak etter personregisterloven § 22 første ledd.

Det samme gjelder når et forvaltningsorgan bearbeider opplysninger for kollegiale organer, sakkyndige eller tilsynsførere m.v. som er tilknyttet etaten, eller for private som er engasjert for å løse oppgaver for etaten.

§ 5-2

Et forvaltningsorgan som bearbeider personopplysninger som det har mottatt fra andre forvaltningsorganer, regnes ikke som databehandlingsforetak etter personregisterloven § 22 første ledd dersom bearbeidingen hovedsaklig skjer ut fra organets eget behov, eller for slike organer som nevnt ovenfor i § 5-1. Dette gjelder selv om bearbeidede opplysninger sendes tilbake til det organ som forvaltningsorganet mottok opplysninger fra.

§ 5-3

Datatilsynet gis myndighet til ved enkeltvedtak å gjøre unntak fra de enkelte bestemmelser i personregisterloven kap. 6, jfr. loven § 22 tredje ledd.

§ 5-4

Datatilsynet gis myndighet til ved enkeltvedtak å gi bestemmelser som nevnt i personregisterloven § 24 annet ledd.

KAPITTEL 6

KONSESJON FOR ADRESSERINGS- OG DISTRIBUSJONSVIRKSOMHET

(Personregisterloven §§ 25,26 og 29)

§ 6-1

Reglene i kapittel 7 i personregisterloven gjelder ikke for virksomhet drevet av forvaltningsorganer (jfr. forvaltningsloven § 1).

§ 6-2

Datatilsynet gis myndighet til ved enkeltvedtak å gjøre slike unntak som nevnt i personregisterloven § 25 annet ledd.

§ 6-3

Datatilsynet gis myndighet til ved enkeltvedtak å gi regler som nevnt i personregisterloven § 26 annet ledd.

§ 6-4

For å gjennomføre reglene i personregisterloven § 28 må foretaket opprette et eget register over eller på annen måte anmerke de personer som etter lovens § 28 krever seg slettet blant de adresser foretaket tilbyr eller benytter, slik at de som har krevd seg slettet, ikke lenger står som adressat på de utskrifter som foretaket tilbyr eller benytter til distribusjon.

Når foretaket har mottatt krav om sletting, skal det bare oppbevare de opplysninger om vedkommende som er nødvendig for å hindre at vedkommende kommer med en adressatutskrift.

Tiltak etter første og annet ledd skal foretas innen en frist som fastsettes ved den enkelte konsesjon.

§ 6-5

Datatilsynet gis myndighet til ved enkeltvedtak å gi slike regler som nevnt i personregisterloven § 29.

§ 6-6

I medhold av personregisterloven § 30 nr. 1 bestemmes at lovens § 28 skal gjelde også for foretak som i enkeltstående tilfeller påtar seg oppdrag som nevnt i lovens § 25 første ledd.

I medhold av personregisterloven § 30 nr. 2 bestemmes at lovens § 28 skal gjelde også for adresselister til bruk for utsending av et foretaks egne varer og tjenester o.l.

KAPITTEL 7

(Personregisterloven §§ 31 og 35.)

§ 7-1

Et forvaltningsorgan (jfr. forvaltningslovens § 1) som utfører opinions- eller markedsundersøkelser for andre over-, under eller sideordnede organer i samme etat, trenger ikke konsesjon etter personregisterloven § 31 første ledd.

Det samme gjelder når et forvaltningsorgan utfører opinions- eller markedsundersøkelser for kollegiale organer, sakkyndige eller tilsynsførere m.m., som er tilknyttet etaten, eller for private som er engasjert for på løse oppgaven for etaten.

§ 7-2

Et forvaltningsorgan som utfører opinions- eller markedsundersøkelser ved hjelp av opplysninger det har mottatt fra andre forvaltningsorganer, trenger ikke konsesjon etter personregisterlovens § 31 første ledd, dersom undersøkelsen hovedsaklig skjer ut fra organets egne behov, eller for slike organer som nevnt ovenfor i § 7-1. Dette gjelder selv om bearbeidede opplysninger sendes tilbake til det organ som forvaltningsorganet mottok opplysning fra.

§ 7-3

Datatilsynet gis myndighet til ved enkeltvedtak å gjøre unntak fra de enkelte bestemmelser i personregisterloven kap. 8, jfr. lovens § 31 annet ledd.

§ 7-4

I henhold til personregisterloven § 35 bestemmes at lovens §§ 32 til 34 også skal gjelde for foretak som i enkeltstående tilfeller påtar seg slike oppdrag som nevnt i lovens § 31 første ledd, og for foretak som setter i verk slike undersøkelser for sin egen administrasjon og virksomhet.

KAPITTEL 8

SAMTYKKE TIL OVERFØRING TIL UTLANDET

(Personregisterloven § 36 tredje ledd.)

§ 8-1

Dersom register eller opplysning som nevnt i lovens § 36 første og annet ledd overføres til utlandet, behøves ikke slikt samtykke som nevnt i § 36. Overføring må meldes til Datatilsynet i god tid før overføring finner sted. Datatilsynet kan nekte overføring eller sette vilkår for overføringen.

Overføring behøver ikke meldes når Norge har plikt til å foreta slik overføring etter folkerettslig overenskomst eller som følge av medlemsskap i internasjonal organisasjon.

KAPITTEL 9

STRAFFEBESTEMMELSER

(Personregisterloven § 38 tredje ledd.)

§ 9-1

Den som forsettlig eller aktløst unnlater å følge reglene i disse forskrifter § 1-1, § 1-2, § 1-3, § 2-1, § 4-3 eller § 8-1, straffes med bøter eller fengsel inntil ett år eller begge deler.

Medvirkning straffes på samme måte.

COUNCIL OF EUROPE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

FINAL DRAFT APPROVED BY EUROPEAN COMMITTEE ON LEGAL COOPERATION, 27 JUNE 1980 AND PRESENTED TO COUNCIL OF MINISTERS FOR ADOPTION

PREAMBLE

The Member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its Members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms,

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing,

Reaffirming at the same time their commitment to freedom of information regardless of frontiers,

Recognizing that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:

CHAPTER I - GENERAL PROVISIONS

Article 1 - Object and purpose

The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection').

Article 2 - Definitions

For the purpose of this Convention:

a) 'personal data' means any information relating to an identified or identifiable individual ('data subject');

b) 'automated data file' means any set of data undergoing automatic processing,

c) 'automatic processing' includes the following operations if carried out in whole or in part by automated means: storage of data; carrying out of logical and/or arithmetical operations on those data; their alteration, erasure, retrieval or dissemination;

d) 'controller of the file' means the natural or legal person, public authority, agency or any other body who is competent according to his national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which processes should be applied to them

Article 3 - Scope

1 The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors.

2 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe

a) that it will not apply this Convention to certain categories of automated personal data files, a list of which will be deposited In this list it shall not include, however, categories of automated data files subject in its domestic law to data protection provisions Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions in its domestic law,

b) that it will apply this Convention also to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;

c) that it will apply this Convention also to personal data files which are not processed automatically

3 Any State which has extended the scope of the Convention by any of the declarations provided for in sub-paragraph 2(b) or (c) above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited

4 Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2(a) above may not claim the application of this Convention to such categories by a Party which has not excluded them.

5 Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraph 2(b) and (c) above may not claim the application of this Convention on these points with respect to a Party which has made such extensions.

6 The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the Convention with regard to the State which has made them at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been formulated at any later time. These declara-

tions may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

CHAPTER II - BASIC PRINCIPLES FOR DATA PROTECTION

Article 4 – Duties of the Parties

1 Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2 These measures shall be taken at the latest at the time of entry into force of this Convention in respect of that Party.

Article 5 – Quality of data

Personal data undergoing automatic processing shall be:

a) obtained and processed fairly and lawfully;

b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c) adequate, relevant and not excessive in relation to the purpose for which they are stored;

d) accurate and, where necessary, kept up-to-date;

e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6 - Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7 - Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.

Article 8 - Additional safeguards for the data subject

Any person shall be enabled:

a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;

d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs (b) and (c) of this article is not complied with.

Article 9 – Exceptions and restrictions

1 No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article.

2 Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed where such derogation provided for by the law of the Party constitutes a necessary measure in a democratic society in the interests of:

a) protecting state security, public safety, the monetary interests of the State or the suppression of criminal offences;

b) protecting the data subject or the rights and freedoms of others.

3 Restrictions on the exercise of the rights specified in Article 8, paragraphs (b), (c) and (d) may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10 – Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11—Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this Convention.

CHAPTER III - TRANSBORDER DATA FLOWS

Article 12 – Transborder flows of personal data and domestic law

1 The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

2 A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party.

3 Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:

a) insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;

b) when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

CHAPTER IV—MUTUAL ASSISTANCE

Article 13 – Cooperation between Parties

1 The Parties agree to render each other mutual assistance in order to implement this Convention.

2 For that purpose:

a) each Party shall designate one or more authorities the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;

b) each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority

3 An authority designated by a Party shall at the request of an authority designated by another Party:

a) furnish information on its law and administrative practice in the field of data protection;

b) for the sole purpose of protection of privacy, take all appropriate measures, in conformity with its domestic law, for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed

Article 14 – Assistance to data subjects resident abroad

1 Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this Convention

2 When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.

3 The request for assistance shall contain all the necessary particulars, relating inter alia to:

a) the name, address and any other relevant particulars identifying the person making the request;

b) the automated personal data file to which the request pertains, or its controller,

c) the nature of the request.

Article 15 – Safeguards concerning assistance rendered by designated authorities

1 An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.

2 Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate restrictions of secrecy or confidentiality with regard to that information.

3 In no case may a designated authority be allowed to make a request for assistance on behalf of a data subject resident abroad, as referred to in Article 14, paragraph 2 of its own accord and without the express consent of the person concerned.

Article 16 – Refusal of requests for assistance

A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this Convention may not refuse to comply with it unless:

a) the request is not compatible with the powers in the field of data protection of the authorities responsible for replying,

b) the request does not comply with the provisions of this Convention;

c) compliance with the request would be incompatible with the sovereignty, security or public policy (ordre public) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party

Article 17 – Costs and procedures of assistance

1 Mutual assistance which the Parties render each other under Article 13, and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.

2 The data subject may be charged no costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party

3 Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

CHAPTER V – CONSULTATIVE COMMITTEE

Article 18—Composition of the Committee

1 A Consultative Committee shall be set up after the entry into force of this Convention.

2 Each Party shall appoint a representative to the Committee and a deputy representative Any Member State of the Council of Europe which is not a Party to the Convention shall have the right to be represented on the Committee by an observer

3 The Consultative Committee may, by unanimous decision, invite any non-Member State of the Council of Europe which is not a Party to the Convention to be represented by an observer at any of its meetings.

Article 19 – Functions of the Committee

The Consultative Committee:

a) may make proposals with a view to facilitating or improving the application of the Convention;

b) may make proposals for amendment of this Convention in conformity with Article 21;

c) shall formulate its opinion on any proposal for amendment of this Convention which is referred to it in conformity with Article 21, paragraph 3;

d) may, at the request of a Party, express an opinion on any question concerning the application of this Convention

Article 20 – Procedure

1 The Consultative Committee shall be convened by the Secretary General of the Council of Europe Its first meeting shall be held within twelve months of the entry into force of

this Convention. It shall subsequently meet at least once every two years and in any case when one third of the representatives of the Parties request its convocation.

2 A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.

3 After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the Convention.

4 Subject to the provisions of this Convention, the Consultative Committee shall draw up its own Rules of Procedure.

CHAPTER VI – AMENDMENTS

Article 21 – Amendments

1 Amendments to this Convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.

2 Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the Member States of the Council of Europe and to every non-Member State which has acceded to or has been invited to accede to this Convention in accordance with the provisions of Article 23.

3 Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee which shall submit to the Committee of Ministers its opinion on that proposed amendment.

4 The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.

5 The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.

6 Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

CHAPTER VII – FINAL CLAUSES

Article 22 – Entry into force

1 This Convention shall be open for signature by the Member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

2 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five Member States of the Council of Europe have expressed their consent to be bound by the Convention in accordance with the provisions of the preceding paragraph.

3 In respect of any Member State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the deposit of the instrument of ratification, acceptance or approval.

Article 23 – Accession by non-Member States

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this Convention by a decision taken by the majority provided by Article 20(d) of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee.

2 In respect of any acceding State, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of ratification with the Secretary General of the Council of Europe.

Article 24 – Territorial clause

1 Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt by the Secretary General of such declaration.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 25 – Reservations

No reservation may be made in respect of the provisions of this Convention.

Article 26 – Denunciation

1 Any Party may at any time denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 27 – Notifications

The Secretary General of the Council of Europe shall notify the Member States of the Council and any State which has acceded to this Convention of:

a) any signature,

b) the deposit of any instrument of ratification, acceptance, approval or accession,

c) any date of entry into force of this Convention in accordance with Articles 22, 23 and 24;

d) any other act, notification or communication relating to this Convention. ■

VEDLEGG 5: OECD's retningslinjer for beskyttelse av personvern og fri flyt av persondata over landegrenser

OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

RECOMMENDATION OF THE COUNCIL OF EUROPE ADOPTED AT ITS 523RD MEETING ON 23 SEPTEMBER 1980*

The Council,

Having regard to Articles 1(c), 3(a) and 5(b) of the Convention of the Organization for Economic Cooperation and Development of 14 December 1960;

Recognizing:
– that, although national laws and policies may differ, member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;
– that automatic processing and transborder flows of personal data create new forms of relationship among countries and require the development of compatible rules and practices;
– that transborder flows of personal data contribute to economic and social development;
– that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows,

Determined to advance the free flow of information between member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among member countries;

RECOMMENDS

1 That member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;

2 That member countries endeavor to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;

3 That member countries cooperate in the implementation of the Guidelines set forth in the Annex;

4 That member countries agree as soon as possible on specific procedures of consultation and cooperation for the application of these Guidelines.

Annex

PART ONE - GENERAL

Definitions

1 For the purposes of these Guidelines:
a) 'data controller' means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;
b) 'personal data' means any information relating to an identified or identifiable individual (data subject);
c) 'transborder flows of personal data' means movements of personal data across national borders

Scope of Guidelines

2 These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties

3 These Guidelines should not be interpreted as preventing
a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
c) the application of the Guidelines only to automatic processing of personal data

4 Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy (*ordre public*), should be:
a) as few as possible, and
b) made known to the public

5 In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6 These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO - BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection limitation principle

7 There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data quality principle

8 Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose specification principle

9 The purposes for which personal data are collected should be specified not later than at the time of data collection and

* The Australian, Canadian, Irish, Turkish and United Kingdom Governments abstained

the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use limitation principle

10 Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except

a) with the consent of the data subject; or

b) by the authority of law

Security safeguards principle

11 Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness principle

12 There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual participation principle

13 An individual should have the right

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him,

b) to have communicated to him, data relating to him

i) within a reasonable time,

ii) at a charge, if any, that is not excessive,

iii) in a reasonable manner; and

iv) in a form that is readily intelligible to him,

c) to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial, and

d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability principle

14 A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE – BASIC PRINCIPLES OF INTERNATIONAL APPLICATION FREE FLOW AND LEGITIMATE RESTRICTIONS

15 Member countries should take into consideration the implications for other member countries of domestic processing and re-export of personal data.

16 Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a member country, are uninterrupted and secure.

17 A member country should refrain from restricting transborder flows of personal data between itself and another member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other member country provides no equivalent protection.

18 Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR – NATIONAL IMPLEMENTATION

19 In implementing domestically the principles set forth in Parts Two and Three, member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavor to

a) adopt appropriate domestic legislation,

b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise,

c) provide for reasonable means for individuals to exercise their rights,

d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three, and

e) ensure that there is no unfair discrimination against data subjects.

PART FIVE – INTERNATIONAL COOPERATION

20 Member countries should, where requested, make known to other member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other member countries which comply with these Guidelines.

21 Member countries should establish procedures to facilitate

a) information exchange related to these Guidelines; and

b) mutual assistance in the procedural and investigative matters involved.

22 Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data. ■

ISBN 82-00-06552-9

LOBO, Oslo