Innst. 270 S

(2012–2013)

**Innstilling til Stortinget
fra kommunal- og forvaltningskomiteen**

Meld. St. 11 (2012–2013)

Innstilling fra kommunal- og forvaltningskomiteen om personvern – utsikter og utfordringar

Innhold

Innst. 270 S

(2012–2013)

**Innstilling til Stortinget
fra kommunal- og forvaltningskomiteen**

Meld. St. 11 (2012–2013)

Innstilling fra kommunal- og forvaltningskomiteen om personvern – utsikter og utfordringar

Til Stortinget

1. Innleiing

1.1 Sammendrag

I meldinga blir det peikt på at behandling og utveksling av personopplysningar er ein nødvendig føresetnad i eit moderne samfunn. Ulike teknologiske løysingar for behandling av personopplysningar legg til rette for gode, sikre og lett tilgjengelege tenester for innbyggjarane. Regjeringa ønskjer å digitalisere forvaltninga og dei tenestene forvaltninga yter til innbyggjarane, og har som mål at dette skal gi betre og meir tilgjengelege tenester. Også i privat sektor er mange tenester digitaliserte ved at kundane har tilgang til elektroniske innsynsløysingar, elektroniske skjema og så vidare. Personvern er eit av omsyna ein må leggje vekt på når ein tek i bruk teknologi i tenesteytinga. Bruk av teknologi gjer det mogleg å ta vare på personvernet på nye måtar.

Det blir i meldinga vist til at samfunnet er avhengig av god bruk og flyt av personopplysningar. Dette gagnar òg innbyggjarane. Det norske personvernregelverket gjennomfører EUs personverndirektiv frå 1995, og personvernlovgivinga vår liknar derfor i grove trekk på personvernlovgivinga i medlemsstatane i EU. EUs personvernregelverk har som eit viktig mål å leggje til rette for fri flyt av personopplysningar som grunnlag for utvikling og vekst i den indre marknaden. Bruk av personopplysningar er ein av mange føresetnader for eit velfungerande samfunn, både i offentleg og privat verksemd.

1.1.1 Rapporten frå Personvernkommisjonen, bakgrunnen for og målet med denne meldinga frå regjeringa til Stortinget

St.meld. nr. 17 (2006–2007) Eit informasjonssamfunn for alle seier mange stader at ein må sjå personvernet i ein heilskapleg samanheng, og i punkt 8.3.1 i meldinga vart det gjort framlegg om å setje ned ein personvernkommisjon. Framlegget om å nemne opp ein personvernkommisjon vart behandla våren 2006, og framlegget fekk støtte frå eit samla Storting. Personvernkommisjonen vart oppnemnd av regjeringa 25. mai 2007.

Rapporten er innteken i NOU 2009:1 Individ og integritet – Personvern i det digitale samfunnet (heretter omtala som PVK-rapporten eller rapporten frå Personvernkommisjonen).

Kommisjonen vart særleg beden om å kome med tilrådingar til betre personvern på desse fem konkrete områda: media, barn og unge, arbeidslivet, helsesektoren og transport- og kommunikasjonssektoren. Som supplement til temaa i mandatet har Personvernkommisjonen gjort greie for ulike teknologiar som har konsekvensar for personvernet og utviklinga på teknologiområdet. Dette gir eit nyttig bakteppe for mange av vurderingane frå kommisjonen. Kommisjonen har vidare drøfta spørsmål knytte til oppgåvene til og organiseringa av tilsynsstyremakta og spørsmål om grunnlovsfesting av personvernet. Rapporten frå Personvernkommisjonen var på brei høyring i 2009, og det kom inn mange og gode innspel til vidare arbeid på personvernområdet.

Meld. St. 11 (2012–2013) byggjer på mange av funna frå arbeidet Personvernkommisjonen gjorde, og på innspela frå høyringsrunden. I samband med behandlinga av innstilling til Stortinget om gjennomføring av EUs datalagringsdirektiv, bad Stortinget om nærmare utgreiing av fleire tema på personvern-

området. Dette gjeld krav til logging, gjennomgang av rutinar for å sikre teieplikta i Arbeids- og velferdsetaten og ordninga med personvernombod. Desse temaa blir omtalte i meldinga.

Meldinga byggjer òg på det som er sagt i Soria Moria-erklæringa om varetaking av personvernomsyn.

1.1.2 Avgrensing mot delar av rapporten frå Personvernkommisjonen

1.1.2.1 Strukturen i rapporten – korleis regjeringa vurderer einskilde tiltak

Sjølv om regjeringa ikkje tok sikte på å gå gjennom alle framlegga frå Personvernkommisjonen blir det likevel i meldinga kort gjort greie for korleis regjeringa allereie har følgt opp fleire av framlegga frå Personvernkommisjonen på ulike område, sjå kapittel 2.3. Meldinga gjer òg greie for korleis nokre framlegg er vurderte utan at det er funne grunnlag for å gå vidare med dei. Regjeringa ønskjer likevel eit ordskifte på eit meir overordna nivå enn det Personvernkommisjonen konkret har greidd ut og kome med framlegg om. Det blir vist til at det derfor ikkje er eit mål at alle framlegga frå kommisjonen skal omtalast i denne meldinga. Meldinga tek heller ikkje sikte på å gjere greie for status for personvernet i dei ulike sektorane som Personvernkommisjonen har skrive om i rapporten sin.

Personvernkommisjonen gjer i rapporten sin punkt 13.5.3 framlegg om at ordninga med fri rettshjelp skal utvidast til å femne om visse saker mot media. Det blir i meldinga peikt på at behovet for endringar i rettshjelpsordninga vart gjennomgått og vurdert i St.meld. nr. 26 (2008–2009) Om offentleg rettshjelp. Der vart det konkludert med at ordninga ikkje skal femne om rettsleg prøving av personvernkrenkingar som media har gjort seg skuldige i.

Det blir i meldinga vist til at Personvernkommisjonen gjer framlegg om ei rad tiltak som kan betre personvernet til pasientane i helsesektoren. Eitt av framlegga frå kommisjonen var mellombels stopp i etableringa av nye helseregister i påvente av ein gjennomgang og ei evaluering av registra som finst i dag. Regjeringa meiner dette ikkje er eit nødvendig tiltak, og framlegget frå Personvernkommisjonen om eit moratorium mot å opprette nye helseregister i påvente av ein gjennomgang av eksisterande register blir derfor ikkje nærmare drøfta i meldinga. Det blir i meldinga peikt på at det alltid blir gjort grundige personvernvurderingar i samband med oppretting av nye eller endring av eksisterande helseregister. Det blir heller ikkje oppretta nye helseregister utan at behovet er grundig utgreidd og dokumentert. Etter at kommisjonen kom med rapporten sin, har Stortinget mellom anna gjort vedtak om å opprette eit nasjonalt register over hjarte- og karlidingar, sentralt helsearkivregister og nasjonal kjernejournal. Dette syner at det er brei semje om at ein treng sentrale helseregister for å ivareta ein del viktige helserelaterte oppgåver.

1.1.2.2 Grunnlovsfesting av personvern

Grunnlovsfesting av personvernet kan synleggjere personvernet som menneskerett og kva rom denne retten bør ha i samfunnet vårt. Personvernkommisjonen konkluderer i rapporten sin med at retten til personvern bør grunnlovsfestast i Noreg.

Grunnlovsfesting av menneskerettar er òg vurdert av det stortingsoppnemnde Menneskerettsutvalet. Utvalet leverte rapporten sin 10. januar 2012. I meldinga kap. 2.2.2 blir det gitt utdrag frå rapporten.

Det blir i meldinga vist til at grunnlovsfesting av retten til personvern ikkje endrar rettstilstanden slik han er i dag, men strekar under kor viktig denne retten er. Når det gjeld andre vurderingar av behovet for og konsekvensane av grunnlovsfesting av retten til personvern, blir det vist til dei nemnde dokumenta.

Regjeringa ser det slik at ein bør behandle spørsmålet om grunnlovsfesting av personvernet saman med spørsmålet om grunnlovsfesting av andre menneskerettar. Det er riktig og føremålstenleg å gjere ei samla og heilskapleg vurdering av framlegga og tilrådingane frå Menneskerettsutvalet. Det blir i meldinga vist til at regjeringa derfor ikkje vil gjere ytterlegare vurderingar av spørsmålet om grunnlovsfesting av personvernet i meldinga.

1.1.3 Tilrådingane frå Personvernkommisjonen – gjennomførte tiltak

Det blir i meldinga vist til at rapporten frå Personvernkommisjonen inneheld eit breitt spekter av vel tufta framlegg til betre varetaking av personvernet i eit samfunn med rivande teknologisk utvikling. Mange av framlegga frå kommisjonen er allereie gjennomførte.

Personvern og medium

I vurderinga av personvernutfordringar som oppstår når folk møter og bruker ulike medium, peiker Personvernkommisjonen på ei rad moglege tiltak som kan betre integritetsvernet. Eit viktig tiltak regjeringa har sett i gang, er drifta av slettehjelpstenesta slettmeg.no. Frå 1. januar 2012 har tenesta vore driven av NorSIS. Tenesta er eit døme på eit særs vellukka lågterskeltilbod som har gitt verdfull hjelp utan å vurdere om ytringar er rette eller galne, lovlege eller ulovlege.

Eit anna viktig tiltak Personvernkommisjonen gjorde framlegg om for å betre integritetsvernet i media, var å setje grenser både for publikum og for media når det gjeld å søkje og stille saman opplysningar frå skattelistene. Gode grunnar tala for ei inn-

stramming på dette området, og regjeringa la i mai 2011 fram Prop. 116 LS (2010–2011) om mellom anna innstrammingar i reglane om innsyn i skattelistene. Saka vart behandla i Stortinget i juni 2011, og det vart vedteke å endre praksis for offentleggjering av skattelistene.

PERSONVERN I ARBEIDSLIVET

Bruken av teknologi i arbeidslivet aukar sterkt. Forskrifter om innsynet arbeidsgivaren har i e-posten til dei tilsette, vart vedtekne i personopplysningsforskrifta 29. januar 2009 og tok til å gjelde 1. mars same året.

PERSONVERN I HELSESEKTOREN

I gjennomgangen av personvernutfordringar i helsesektoren peiker Personvernkommisjonen på ei rad moglege tiltak. Kommisjonen gjer framlegg om at pasienten bør ha rett til å reservere seg mot innsyn i den elektroniske pasientjournalen sin på tvers av verksemder, og at kvar einskild bør ha innsynsrett i tilgangsloggen til pasientjournalen sin. Begge desse framlegga vart vedtekne då helseregisterlova vart endra 19. juni 2009.

BARN OG PERSONVERN

Personopplysningslova vart revidert våren 2012. Mellom anna vart det vedteke ein særskild regel i personopplysningslova § 11 siste leddet som skal gi betre personvern for barn. Den nye regelen inneber eit styrkt vern, fordi personopplysningar om barn ikkje kan behandlast dersom dette er uforsvarleg med tanke på det beste for barnet. I tillegg kan Datatilsynet gripe inn ved grove krenkingar av personvernet til barn. Lovvedtaket legg til rette for betre varetaking av personvernet for barn generelt.

1.1.4 Avgrensing mot igangsett arbeid med personvernkonsekvensar

1.1.4.1 ARBEIDSLIV

Personvern i arbeidslivet handlar om å vege behovet arbeidsgivaren har for å kontrollere kva som går føre seg i verksemda, mot behovet arbeidstakaren har for vern av personleg integritet og personlege opplysningar.

Reglar om kontroll og overvaking i arbeidslivet vart lovfesta i kapittel 9 i arbeidsmiljølova i 2005. Etter kvart som problemstillinga kring retten arbeidsgivaren har til innsyn i e-post vart meir og meir aktuell, vart det klårt at dei rettslege standardane på området trong utdjuping og konkretisering. Dette vart derfor nærmare regulert i kapittel 9 i personopplysningsforskrifta i januar 2009. Det viste seg etter kvart at reint privatrettsleg handheving av kontroll- og overvakingskapittelet i arbeidsmiljølova ikkje var særleg praktisk. Frå 1. januar 2010 fekk derfor Arbeidstilsynet handhevingsmyndigheit for reglane i kapittel 9 i arbeidsmiljølova.

I tillegg finst det no ein del rettspraksis som gjer det mogleg å sjå nokre tendensar for korleis lovverket fungerer. Det ligg òg føre ein del forskingsrapportar om emnet.

Vinteren 2011–2012 sette Arbeidsdepartementet ned ei arbeidsgruppe for å vurdere om det trengst tiltak for å betre personvernet i arbeidslivet. Nett no har ein ikkje noko klårt bilete av kva utfordringar som ligg føre, omfanget av utfordringane og behovet for tiltak. Samstundes synest det som nokre bransjar har ei urovekkjande utvikling, både når det gjeld arbeidsmiljø og personvern.

1.1.4.2 BARNE- OG LIKESTILLINGSSEKTOREN

Barne-, likestillings- og inkluderingsdepartementet arbeider med reglar om openheit kring løn som eit tiltak for likeløn og mot lønsdiskriminering. Personvernomsyn er eit tema i regelverksarbeidet, og framlegga er utforma i samsvar med reglane i personopplysningslova og prinsippa som følgjer av denne meldinga.

I 2006 bad Stortinget regjeringa om å greie ut spørsmålet om ein bør opprette eit register over gjeld i Noreg, jf. Dokument nr. 8:95 (2005–2006) om tiltak for å motverke fattigdom og førebyggje gjeldsproblem og Innst. S. nr. 120 (2006–2007). Barne-, likestillings- og inkluderingsdepartementet greier ut alternative modellar for korleis tilgangen til opplysningane skal innrettast, og tek sikte på å sende ut eit høyringsnotat om saka hausten 2012.

Etablering av eit system for registrering og bruk av opplysningar om usikra forbrukskreditt gir likevel utfordringar når det gjeld personvernet. I arbeidet som er i gang, blir det vurdert ulike tiltak for å sikre tilfredsstillande varetaking av sentrale personvernomsyn i samband med gjeldsregistrering.

1.1.4.3 FINANSSEKTOREN

I Finansdepartementet går det føre seg eit større lovarbeid på bank- og forsikringsområdet. Banklovkommisjonen kom 27. mai 2011 med si utgreiing nr. 24, NOU 2011:8 med utkast til lov om finansføretak og finanskonsern m.m. (finansføretakslova). Banklovkommisjonen har laga utkast til ny finansføretakslov som kan avløyse det meste av gjeldande lover på bank- og forsikringsområdet. Personvernomsyn er relevante i tilknyting til fleire av dei spørsmåla som Banklovkommisjonen drøftar i utgreiinga si. Finansdepartementet arbeider for tida med ein lovproposisjon til Stortinget som følgjer opp utgreiinga frå Banklovkommisjonen.

1.1.4.4 Helse- og omsorgssektoren

I helse- og omsorgssektoren er arbeid med personvern, til liks med betring av tenestetilbodet, kontinuerlege prosessar. Parallelt med personvernmeldinga har regjeringa fremja to meldingar til Stortinget, ei om digitale tenester i helse- og omsorgssektoren (e-helse) og ei om kvalitet og pasienttryggleik, der personvern òg er eit viktig element. Spesifikke personvernutfordringar knytte til desse temaa blir derfor ikkje omtala i Meld. St. 11 (2012–2013).

Samhandlingsreforma og fokuset på føresetnaden om ein heilskapleg pasientgang demokratiserer helsetenesta ved å involvere brukarar og pasientar i større grad enn i dag. Det inneber mellom anna at ein må satse sterkt på digitale tenester, der pasienten i mykje større grad skal få tilgang til informasjon om sitt eige pasientforhold.

I NOU 2011:11 Innovasjon i omsorg, drøftar utvalet bruk av sporings- og varslingsteknologi i omsorgssektoren sett i lys av personvernspørsmål. Forslag til endringar av korleis ein kan bruke varslings- og lokaliseringsteknologi, er allereie sende på høyring.

Det går jamleg føre seg opplærings- og haldningsskapande tiltak som skal sikre at teieplikta blir ivareteken. Elles må utdannings- og opplæringstilbodet for helse- og omsorgspersonell spegle den elektroniske kvardagen dei arbeider i, og korleis elektronisk samhandling påverkar helse- og omsorgstenesta.

Det er i gang eit arbeid med revisjon av helseregisterlova. Samstundes blir det arbeidd med organisering og strukturering av nasjonale helseregister for å leggje til rette for betre utnytting, betre kvalitet og endå sikrare handtering av data. Personvernomsyn står sentralt i dette arbeidet.

1.1.4.5 Justissektoren

Delrevisjon av personopplysningslova

I Prop. 47 L (2011–2012) vart det føreslått reglar som skal oppdatere personopplysningslova på område der det har vist seg at det trengst endringar. Endringane vart vedtekne 27. mars 2012 og sette i kraft 20. april 2012.

Ivaretaking av personvernet for barn er eit hovudtema i rapporten frå Personvernkommisjonen. Då personopplysningslova vart endra i 2012, vart det innført ein særskild regel om personvern for barn i § 11 siste leddet. Den nye lovregelen inneber eit styrkt vern for barn ved å slå fast at ein ikkje kan behandle personopplysningar om barn dersom dette er uforsvarleg med tanke på det beste for barnet. I tillegg kan Datatilsynet gripe inn ved grove krenkingar av personvernet til barn.

Reglane om kameraovervaking er moderniserte. Definisjonen av kameraovervaking er gjord meir tidsriktig, og dei same reglane skal gjelde for bruk av falske kameraløysingar (dummykamera) som for ordinære overvakingskamera. Det er innført strengare reglar for overvaking i somme rekreasjonsområde i tillegg til ei plikt til å varsle dersom det parallelt med kameraovervakinga blir gjort lydopptak.

Det er òg vedteke ei forenkling av konsesjonsordninga for behandling av sensitive personopplysningar.

Personopplysningslova § 7 om tilhøvet mellom personvernet og ytringsfridomen er endra. Før endringa kunne det gjerast unntak frå dei mest sentrale reglane i personopplysningslova dersom personopplysningar vart behandla «utelukkende for kunstneriske, litterære eller journalistiske, herunder opinionsdannende formål». Uttrykket «opinionsdannende» har skapt tolkingstvil og utfordringar. Det er no fjerna frå lovregelen, slik at rekkevidda av unntaket blir klårgjord.

Når nye EU-reglar blir vedteke, trengst det venteleg fleire endringar i den norske personvernlovgivinga, og ein meir vidfemnande etterkontroll av personopplysningslova kan derfor gjennomførast i samband med gjennomføringa av EU-reglane i norsk rett. Meldinga tek derfor ikkje sikte på å greie ut om det trengst endringar i den gjeldande personopplysningslova.

Schengen-samarbeidet

Noreg har sidan 2001 vore part i Schengen-samarbeidet og skal føre ein harmonisert visum- og grensekontrollpolitikk. Biometriske kjenneteikn i form av fotografi og fingeravtrykk er gradvis innførte på visumområdet og i grensekontrollen. I 2011 vart Visa Information System (VIS) teke i bruk. VIS er eit felles datasystem for Schengen-medlemslanda.

Ved utviklinga av regelverk innan Schengensamarbeidet legg EU-kommisjonen og Schengenmedlemslanda EUs gjeldande regelverk om personvern til grunn og konsulterer jamleg EU-komiteen med ansvar for personvern. VIS blir rekna for å vere i tråd med norsk personvernregelverk og er implementert i utlendingslova §§ 102 a til 102 f.

Behandling av personopplysningar i kriminalomsorga – forskrifter til straffegjennomføringslova

Straffegjennomføringslova kapittel 1 a om behandling av personopplysningar i kriminalomsorga vart vedteken ved lov 17. desember 2010 nr. 85. Ikraftsetjinga av endringslova er utsett i påvente av at det kjem utfyllande forskrifter. Bakgrunnen for dei nye lovreglane er pålegget frå Datatilsynet om å etablere eit klårare rettsleg grunnlag for behandling av personopplysningar etter tilsynet ved Ila fengsel og forvaringsanstalt i 2007.

Arbeidet med forskrift om behandling av personopplysningar i kriminalomsorga er i gang, og utkastet skal etter planen sendast på høyring hausten 2012 med sikte på at endringslova kan bli sett i kraft i 2013.

INFOFLYT-registeret

Det er nødvendig å utveksle informasjon mellom kriminalomsorga og politiet. For å sikre eit fungerande system vart det i 2005 etablert eit eige informasjonsutvekslingssystem (INFOFLYT) som skulle avdekkje og hindre den mest alvorlege og samfunnsskadelege kriminaliteten.

Sivilombodsmannen har retta kritikk mot INFOFLYT-systemet og peikt på at heimelsgrunnlaget synest uklårt. På bakgrunn av kritikken sette Justis- og politidepartementet i 2010 ned eit utval. Regjeringa vil setje i gang arbeidet med ein proposisjon om endringar i straffegjennomføringslova, slik at INFOFLYT får ei klårare rettsleg forankring. INFOFLYT-rapporten vart send på høyring 27. juni 2012.

Informasjonstrygging og internkontroll i kriminalomsorga

Etter at Datatilsynet gjennomførte tilsyn ved Ila fengsel og forvaringsanstalt hausten 2007, fekk sentralforvaltninga i Kriminalomsorga pålegg om å etablere eit internkontrollsystem for å møte krava i personopplysningslova.

Dette er følgt opp ved at det i 2009 vart utarbeidd ein policy for informasjonstrygging i Kriminalomsorga. I tillegg er det utarbeidd retningsliner både for tilgangsstyring og for logging. I 2010–2011 fekk dei tilsette i Kriminalomsorga omfattande opplæring i det databaserte internkontrollsystemet (KIKS). Alle tilsette har i samband med dette fått opplæring i krava personopplysningslova set til informasjonstryggleik.

1.1.4.6 Utdanningssektoren

Sentralt elevregister

Grunnopplæringa og utdanningsstyremaktene, medrekna Kunnskapsdepartementet og Utdanningsdirektoratet, treng eit godt kunnskapsgrunnlag for å gjere norsk skule betre.

I oktober 2008 sende regjeringa eit framlegg om å etablere eit sentralt individbasert og pseudonymt elevregister i skulesektoren på høyring. Bakgrunnen for framlegget var intensjonen Stortinget har om eit nasjonalt kvalitetsvurderingssystem i skulen som skal nyttast til å rekne ut sentrale kvalitetsindikatorar for kvalitetsutvikling og leggje til rette for styring, forsking og tilsyn. Eit slikt system krev sentral lagring av dei opplysningane som blir samla inn i samsvar med dei fastsette føremåla.

Kunnskapsdepartementet har på bakgrunn av høyringsrunden funne det nødvendig med ytterlegare vurdering av behovet for eit slikt register, eventuelt omfanget av innhaldet og konsekvensar for personvernet. Arbeidet er enno ikkje avslutta.

1.1.4.7 Kultursektoren

Pliktavleveringslova

Kulturdepartementet er i gang med å revidere pliktavleveringslova og skal som eit ledd i denne prosessen mellom anna sjå på korleis ein kan gjennomføre pliktavlevering frå Internett. Dei personvernrelaterte problemstillingane som kan oppstå ved pliktavlevering frå Internett, blir drøfta i revisjonsarbeidet.

Utgreiinga frå Medieansvarsutvalet

Medieansvarsutvalet, som la fram utgreiinga si 15. juni 2011, hadde mellom anna til oppgåve å greie ut:

«Behovet for særskilte lovregler eller tjenester (offentlige eller i regi av mediene selv) som kan sikre enkeltpersoners personvern i møte med media. Utvalget bør særlig vurdere behovet for tiltak overfor nettmedier som ikke har en sentral redaktørfunksjon eller der en privatperson står bak, og der bransjens etiske tilsyns- og klagesystem ikke kommer til anvendelse.»

Korleis regjeringa har følgt opp dette punktet, blir nærmare omtala i kapittel 8 i meldinga.

Når det gjeld dei andre delane av mandatet til utvalet, har regjeringa førebels konkludert med at det framleis bør vere ei særskild regulering av ansvarssystemet for redigerte massemedium. Mellom anna ønskjer regjeringa å halde oppe det formelle straffe-rettslege redaktøransvaret, men i ei meir medieuavhengig form. Det blir nærmare utgreidd av Kulturdepartementet i samråd med dei aktuelle departementa.

1.1.4.8 Samferdselsektoren

Det blir i meldinga vist til at det grovt sett er to tungtvegande samfunnsinteresser som utfordrar personvernet i samferdselssektoren: trafikktryggleik og effektiv og påliteleg framføring av trafikken. Det er eit mål at tiltak for å auke trafikktryggleiken og framføringa av trafikken i minst mogleg grad skal gå ut over retten einskildindividet har til vern om integriteten sin og privatlivet sitt. Personvernet blir òg utfordra innanfor elektronisk kommunikasjon når opplysningar som er lagra for å sikre tryggleik og framføring kan nyttast til andre føremål, som innsatsen mot kriminalitet. Desse spørsmåla er behandla i Prop. 49 L (2010–2011) og ved Stortingets behandling av gjennomføringa av datalagringsdirektivet i norsk rett, Innst. 275 L (2010–2011).

Heilautomatiseringa av innkrevjingsstasjonar krev avvegingar mellom effektivitet, forbrukarinteresser og personvernomsyn. I regi av Samferdselsdepartementet er det sett ned ei arbeidsgruppe som skal sjå på om det er mogleg å få til ei fullgod anonym løysing.

I samband med stortingsbehandlinga av Prop. 49 L om gjennomføring av datalagringsdirektivet i norsk rett og Innst. 275 L (2010–2011) i same saka gjorde Stortinget den 11. april 2011 vedtak nr. 473. I vedtaket går det mellom anna fram at passeringsdata frå bompengeanlegg ikkje skal gjerast kjende for skattestyremaktene før ein kan tilby eit anonymt passeringsalternativ.

Samferdselsdepartementet er involvert i førebuingane til implementering av eCall i Noreg. Dette er ein del av eSafety, eit EU-initiativ som rettar seg mot bruk av IKT for å betre trafikktryggleiken. Enkelt sagt får nye køyretøy installert ein telefon som ringjer nødnummeret dersom bilen er involvert i ei ulukke. Datatilsynet deltek i det nasjonale arbeidet. EU-kommisjonen har som mål at eCall skal vere i drift frå 1. januar 2015. Noreg har forplikta seg til å implementere eCall gjennom eit Memorandum of Understanding som vart signert i 2006.

Lagring av personopplysningar i samband med bruk av elektronisk billettering i kollektivtransporten er omhandla i ei eiga bransjenorm.

1.1.4.9 Teieplikt og opplysningsplikt i førebyggjande verksemd

Teieplikt og personvern heng nøye i hop.

Det går fram i ei rad offentlege dokument at det på fleire samfunnsområde er reist spørsmål om det gjeldande regelverket om teieplikt, opplysingsplikt og -rett er føremålstenleg, og om dette regelverket blir rett praktisert.

Våren 2011 vart det i regi av Justis- og beredskapsdepartementet sett ned ei tverrdepartemental arbeidsgruppe som skal ta føre seg reglane om teieplikt og informasjonsutveksling med tanke på førebygging.

1.1.4.10 IKT-politikken til regjeringa

I april 2012 la regjeringa fram eit program for digitalisering av offentleg sektor (Digitaliseringsprogrammet). Regjeringa vil òg leggje fram ein heilskapleg omtale av IKT-politikken i ei eiga melding til Stortinget. Meldinga om IKT og verdiskaping har eit breiare nedslagsfelt enn offentleg sektor. Personvern er ein viktig faktor for IKT-politikken, både på generelt/overordna nivå og for kvar einskild deltakar, og blir drøfta i IKT-meldinga der det er relevant.

Digitalisering av offentleg forvaltning set personvernet på saklista. Digitaliseringsprogrammet trekkjer opp hovudlinene i politikken regjeringa har for digitalisering av forvaltninga. Regjeringa har som mål at den statlege forvaltninga så langt råd er skal vere tilgjengeleg på nett, og at nettbaserte tenester skal vere hovudforma for kommunikasjon mellom forvaltninga og innbyggjarane og næringslivet.

Digitalisering av offentleg forvaltning skal medverke til at det blir enklare å bruke offentlege tenester. Bruk av personopplysningar på tvers av etatsgrenser, slik at brukarane slepp å gi dei same opplysningane fleire gonger, inneber ein viss gjenbruk av innsamla personopplysningar og krev at regelverket legg til rette for det. Det er sett ned ei tverrdepartemental arbeidsgruppe med deltaking også frå nokre underliggjande etatar som har til mandat å fremje regelverk tilpassa digitalisering. Gruppa skal levere rapporten sin til Fornyings-, administrasjons- og kyrkjedepartementet innan utgangen av 2012.

1.2 Komiteens generelle merknader

Komiteen, medlemmene fra Arbeiderpartiet, Jorodd Asphjell, Lise Christoffersen, Hilde Magnusson, Ingalill Olsen og Eirik Sivertsen, fra Fremskrittspartiet, Gjermund Hagesæter, Morten Ørsal Johansen og Åge Starheim, fra Høyre, Trond Helleland og Michael Tetzschner, fra Sosialistisk Venstreparti, lederen Aksel Hagen, fra Senterpartiet, Heidi Greni, og fra Kristelig Folkeparti, Geir Jørgen Bekkevold, er tilfreds med at en stortingsmelding om personvern fremmes som et grunnlag for diskusjon om utviklingstrekk som kan svekke personvernet, og tiltak som kan gjøres for å bedre datasikkerheten og behandlingen av personlige data. Komiteen er enig med regjeringen når den konstaterer at ved utvikling og innføring av ny teknologi, eller ved igangsetting av tiltak som innebærer behandling av personopplysninger, så er personvernvurderingene sjelden i sentrum. Komiteen slutter seg også til vurderingen av at utredere og beslutningstagere både i privat og offentlig sektor ikke har vurdert personvernkonsekvensene eller satt i verk tiltak som kan ta hensyn til personvernet tidlig nok.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Sosialistisk Venstreparti og Senterpartiet, er tilfreds med at regjeringen i meldingen omhandler de konkrete forslag fra Personvernkommisjonen som allerede er fulgt opp, og i meldingen legger opp til en bred debatt om personvern. Flertallet er opptatt av at spørsmålet om grunnlovfesting av privatlivets fred og personvern-opplysningsvern vurderes i sammenheng med grunnlovfesting av andre menneskerettigheter.

Komiteens medlemmer fra Fremskrittspartiet, Høyre og Kristelig Folkeparti konstaterer at regjeringen velger en mer generell tilnærming enn Personvernkommisjonens områdegjennomgang, og heller vil peke på generelle personvernprinsipper, -mål og -tiltak som en kan tilpasse og bruke på personvernproblemstillinger uansett hvilket samfunnsområde det gjelder.

Disse medlemmer tar til etterretning at regjeringen velger ikke å tilkjennegi sitt syn på eventuell grunnlovfesting av privatlivets fred og personopplysningsvern på det nåværende tidspunkt, men se dette i sammenheng med grunnlovsrevisjon av andre menneskerettigheter.

Komiteens medlemmer fra Høyre og Kristelig Folkeparti vil understreke at grunnlovfesting av personvern ikke bør fremstilles mer komplisert enn det faktisk er, og derfor ikke behøver å bli vurdert sammen med andre forslag som allikevel skal vurderes enkeltvis.

Disse medlemmer mener at en grunnlovfesting vil ha materiell betydning, idet personverninteressen vil bli avveid mot andre rettslige normer av samme trinnhøyde, f.eks. i avveiningen mot Grl. § 100 (ytringsfrihet). Dette er også systematikken i Den europeiske menneskerettighetskonvensjon (EMK), der vernebestemmelser for privatlivet og ytringsfriheten er tatt inn som henholdsvis artikkel 8 og artikkel 10.

Disse medlemmer vil derfor gå inn for grunnlovfesting av personvernet.

Komiteen merker seg med tilfredshet at regjeringen omtaler Personvernkommisjonens forslag om å avgrense tilgjengeligheten av ligningsopplysninger, og at dette ble fulgt opp gjennom Prop. 116 LS (2010–2011).

Komiteen noterer seg likeledes at klargjørende forskrifter om arbeidsgivers innsyn i arbeidstageres e-post ble vedtatt 29. januar 2009.

Komiteen har også merket seg at Personvernkommisjonens forslag om reservasjonsrett mot innsyn i den elektroniske pasientjournalen på tvers av institusjonene og innsynsrett i tilgangsloggen ble innarbeidet i helseregisterloven 19. juni 2009.

Komiteen viser til at regjeringen vil avvente EUs behandling av nye regler om personopplysninger, og at det ventes nye bestemmelser som vil ha følger for den norske personvernlovgivningen, og at meldingen derfor ikke vil vurdere nærmere behovet for endringer i den gjeldende personvernopplysningsloven.

Komiteen har merket seg omtalen av spørsmålet om et sentralt elevregister, og at arbeidet ennå ikke er avsluttet. Komiteen ser frem til at arbeidet sluttføres med tilbørlig sikkerhet for elevdata, og vil i denne forbindelse også fremheve behovet for at elev- og studentopplysninger kan forvaltes uten utleveringsplikt til utenforstående.

Komiteens medlemmer fra Fremskrittspartiet, Høyre og Kristelig Folkeparti viser til at Arbeids- og velferdsforvaltningen har problemer med gamle og utdaterte IKT-systemer. Disse medlemmer har ved flere anledninger uttrykt bekymring for at feilutbetalinger og feil dokumentasjon med personopplysninger er kommet på avveie, noe som har ført til at personvernet for den enkelte har blitt forringet. Disse medlemmer er derfor positive til at denne bekymringen tas til følge ved at det nå rettes en innsats mot å styrke IKT-løsninger og bedre kontrollrutiner ved feilutbetalinger og saksdokumentasjon som er blitt feilsendt til ukjente.

Disse medlemmer viser til at mye av personverndiskusjonen dreier seg om terskelen for å akseptere registrering, f.eks. at den skal begrunnes i et legalt behandlingsformål (grunnlag). Sektororganiseringen i staten innebærer at det er langt flere instanser som til enhver tid vil argumentere for mer registrering av personopplysninger for sin respektive formål, enn de instanser – i praksis ofte bare Datatilsynet – som tar til orde for alternativer, som advarer mot formålsutglidning, som er kritiske til sammenkobling av eksisterende registre og som i det hele utgjør en modererende stemme i koret av krav om flere opplysninger om borgerne.

Disse medlemmer er av den oppfatning at mye av sektorlovgivningen viser at sektororganene ikke selv klarer å avveie personvernhensyn mot påståtte nyttehensyn. Disse medlemmer mener det bør overveies om ikke Justis- og beredskapsdepartementet skal ha det endelige ansvar for å fremme lover initiert av sektordepartementene hvor personvernhensyn er motstående hensyn til de praktiske nyttehensyn som begrunner inngrep i personvernet.

Disse medlemmer fremholder som eksempel på problemet at under arbeidet med meldingen i komiteen har det kommet minst to lovforslag til Stortinget med til dels summarisk drøftelse av forslagenes personvernmessige sider og som setter praktisk nytte for staten foran personvern av borgerne. Det dreier seg om endringer i ekomloven og Prop. 7 L (2012–2013) Endringer i folketrygdloven (tiltak mot misbruk av velferdsordninger).

Disse medlemmer mener det er viktig å foreta grundige avveininger mellom hensynet til personvernet og behovet for å avdekke og forebygge trygdemisbruk. Det er særlig forslaget om registersamkjøring som reiser denne problemstillingen. Disse medlemmer viser til at et av prinsippene

for personvern er at behandling av personopplysninger i størst mulig grad skal være basert på frivillig, uttrykkelig og informert samtykke. I tilfeller hvor det ikke er praktisk eller mulig, må det foreligge et annet rettslig grunnlag. Disse medlemmer mener det er avgjørende at departementet gjennom utformingen av forskrift tar tilstrekkelig hensyn til personvernet, og vil følge med på forslagene fra regjeringen.

Disse medlemmer viser til at sammenstilte masseregistre i andre land også har åpnet for uspesifiserte søk på befolkningskategorier hvor individer tildeles en score rangert ut fra en antatt normaladferd, hvoretter individene som stikker seg ut, blir gjenstand for særskilt kontroll. Forvaltningseksperter har pekt på at slik etterretningsanalyse rettet uspesifisert mot egne borgere uten konkret mistanke, og utenom særhjemmelen som finnes for å beskytte rikets sikkerhet m.m., bryter med prinsippet om informasjon og aktinnsikt. Disse medlemmer vil understreke at det er et lovgiveransvar på ethvert tidspunkt å vurdere utbredelsen av slike metoder, og at en slik praksis som beskrevet ovenfor, i henhold til legalitetsprinsippet ville kreve klar lovhjemmel.

Disse medlemmer viser til at behovet for kontroll med generøse velferdsordninger i andre land har begrunnet analyse- og etterretningsvirksomhet rettet mot egne borgere – både uten konkret mistanke eller med anonyme tips som eneste grunnlag – som ledd i omfattende stikkprøvekontroller. Disse medlemmer viser til at en slik utvikling vil underminere tilliten i samfunnet generelt, og mellom borgerne og forvaltningen. Derimot vil et forhåndssamtykke og informasjon om hvilke kontroller en må godta ved utbetalingen av slike ytelser både være mer opplysende, mer forebyggende, mer skånsomt og et mer effektivt middel mot misbruk, enn å ofre personvernet.

Disse medlemmer viser til at to andre viktige prinsipper for behandling av personopplysninger er formålsbestemthet og proporsjonalitet. Ved registersamkjøring vil opplysninger samlet inn til andre formål brukes til kontroll, noe som er prinsipielt betenkelig. Samtidig er det ikke urimelig at offentlige myndigheter har en anledning til å sjekke reell og faktisk informasjon når en person søker om en offentlig ytelse.

Disse medlemmer mener det er viktig at sensitive personopplysninger holdes utenfor en registersamkjøring.

Disse medlemmer mener blant annet på denne bakgrunn at det også bør innarbeides en positiv lovbestemmelse i norsk forvaltningsrett om forholdsmessighetsprinsippet ved inngrep. Dette innebærer at et forvaltningsvedtak ikke er gyldig når det samfunnet oppnår ved et inngrep overfor den enkelte, ikke er forsvarlig ut fra det som oppnås, eller hvor det samme målet kunne vært oppnådd med mindre inngripende virkemidler.

Disse medlemmer er kjent med at enkelte forvaltningsjurister har søkt å utvikle en forholdsmessighetslære i juridisk teori, men prinsippet er høyst uklart og usikkert uten hjemmel. En lovfesting av forholdsmessighetsprinsippet ville hatt positiv innvirkning på personvernets stilling. En løsning kunne også være å hjemle en proporsjonalitetsnorm i Grunnloven. Disse medlemmer vil under enhver omstendighet komme tilbake til spørsmålet i forbindelse med den pågående diskusjon om modernisering av grunnlovens kapitler om individuelle rettigheter.

Disse medlemmer viser til at personopplysningsloven ikke tillater at personopplysninger lagres lenger enn nødvendig for å gjennomføre formålet med behandlingen. Ofte argumenteres det med at man ønsker å oppbevare opplysningene fordi de kan komme til nytte senere, uten at man nødvendigvis har klart for seg hva man senere skal benytte opplysningene til. I tillegg til at manglende sletting som regel vil være et brudd på personopplysningsloven, øker det også faren for at opplysningene senere kan brukes til andre formål som er uforenlig med det opprinnelige. Disse medlemmer vil fremheve det faktum at passivitet (f.eks. ikke slette når formålet er oppfylt eller bortfalt) er nok til å overtre en rekke bestemmelser i personopplysningsloven, og oppdagelsesrisikoen er forholdsvis begrenset. Derfor er kunnskap om prinsippene vesentlig for de behandlingsansvarlige, sammen med publikums innsynsrett i hva som er lagret og hvilke muligheter man har for sletting, eller i det minste retting.

Komiteens medlemmer fra Fremskrittspartiet og Kristelig Folkeparti er imot datalagringsdirektivet, den svenske FRA-loven og annen lovgivning som innebærer at hele befolkningen i praksis settes under døgnkontinuerlig overvåkning.

Komiteens medlemmer fra Fremskrittspartiet mener dessuten at det bør innføres lovmessig vern av ytringsfrihet og anonymitet på Internett, og viser i den anledning til Dokument 8:55 S (2011–2012) om å lovfeste vern av ytringsfrihet og anonymitet på Internett. Disse medlemmer mener den enkelte skal ha full råderett over sine egne personopplysninger.

Disse medlemmer mener tilliten mellom myndighetene og publikum forringes når personopplysninger kommer på avveie. Disse medlemmer viser til at nettportalen og teknisk plattform for å levere elektroniske skjemaer til det offentlige, Altinn,

har muliggjort at brukere har fått tilgang til andre brukeres personopplysninger også i 2013. Disse medlemmer er bekymret for hva dette gjør med brukernes tillit til elektronisk samhandling med offentlige etater, hvis ikke personopplysninger blir beskyttet på en tilfredsstillende måte.

Disse medlemmer påpeker at offentlig sektors omgang med enkeltmenneskers personopplysninger også i papirformat i enkelte sammenhenger har vært svært risikabel, for eksempel at sensitive personopplysninger og pasientepikriser er blitt overlevert mellom forskjellige instanser innen spesialisthelsetjenesten med taxi, uten at denne informasjonen er blitt fysisk ivaretatt av offentlige tjenestemenn.

Disse medlemmer viser til at politiet per i dag ikke har tilgang til registrene til Nav og Skatt Øst. En som er ettersøkt av politiet kan få midler fra Nav uten at politiet får opplysninger om dette, noe som i praksis kan medføre at staten ettersøker med den ene hånden og gir trygdeytelser med den andre. Disse medlemmer mener også det er et problem i de tilfeller der det er mistanke om trygdemisbruk. Disse medlemmer mener at hensynet til den enkeltes personvern må vike på det tidspunkt man bryter reglene som alle i samfunnet må forholde seg til. Det er viktig for disse medlemmer å understreke at det må foreligge krav om klar mistanke om brudd på offentlige regler, eller mistanke om at straffbare handlinger er begått, ved forespørsel om personlige opplysninger fra andre etater.

Disse medlemmer vil vise til at EØS-borgere som fremviser et skriftlig jobbtilbud, får et registreringsbevis uten sluttdato av Utlendingsdirektoratet (UDI) etter saksbehandling hos politiet. Det er ingen obligatorisk tilbakerapportering til UDI dersom arbeidsforholdet avsluttes. Det siste halve året har norske Nav-kontorer stått overfor følgende dilemma: Nav har ikke mulighet til å stanse støtten til EØS-borgere som de vet bryter kravene til støtte. En ny forskrift gjør at en EØS-borger med jobbkontrakt av minst 14 dagers varighet får et registreringsbevis uten utløpsdato. Når personen i tillegg har fast bopel i Norge, gir dette ham full rett på tjenester som sosialhjelp og kommunal bolig. Det finnes ingen mekanismer for å fange opp at arbeidsforholdet er avsluttet, noe som vil si at beviset er gyldig også etter endt arbeidsforhold. I praksis kan dermed arbeidsinnvandrere som har jobbet i 14 dager kunne heve sosialhjelp, selv om de ansatte i Nav får vite at klienten ikke lenger er i arbeid og dermed ikke har lovlig opphold og rett på støtte. Ifølge regelverket er Nav forhindret fra å overprøve oppholdstillatelse utstedt av UDI. Disse medlemmer viser til at på grunn av taushetsplikten kan Nav heller ikke varsle UDI om klienter som ikke lenger oppfyller kravet til opphold. Disse medlemmer viser for øvrig til Dokument 8:7 S (2012–2013) om at offentlige etater kan utveksle informasjon seg imellom for å avdekke kriminalitet.

Komiteens medlemmer fra Fremskrittspartiet og Høyre er motstandere av gjennomsnittsmåling mellom fotobokser da dette er en farlig form for overvåkning, fordi alle bilistene må registreres og fotograferes, og ikke bare de som kjører for fort. Ved utplassering av tilstrekkelig antall fotobokser vil veimyndighetene kunne følge hver enkelt bil over lange strekninger. Disse medlemmer viser til at Datatilsynet tidligere har sagt nei til gjennomsnittsmåling, og NAF har vært skeptisk av samme grunn. Med kunstig lave fartsgrenser blir gjennomsnittsmåling mellom fotobokser bare nok en avgift som kun har til hensikt å bringe mer penger inn i statskassen. Disse medlemmer mener trafikantene bør følge mer med på trafikkbildet enn på speedometeret, men gjennomsnittsmåling mellom fotobokser kan føre til det motsatte. Disse medlemmer viser til at Datatilsynet i 2006 satte en stopper for totalovervåkning av alle bilister på enkeltstrekninger, og det er skuffende at regjeringen likevel har innført strekningsvis automatisk trafikkontroll. Disse medlemmer vil i den forbindelse vise til tabellen fra Justis- og beredskapsdepartementets svar på budsjettspørsmål nr. 224 fra finanskomiteen/Fremskrittspartiets fraksjon av 8. oktober 2012. Med 5,2 millioner passerte har man allikevel ikke mer enn 25 førerkortbeslag. Disse medlemmer mener den massive overvåkningen ikke står i samsvar til resultatene.

2. Personvern i eit internasjonalt perspektiv

2.1 Sammendrag

2.1.1 Innleiing

Dei internasjonale rettslege instrumenta og det internasjonale samarbeidet på personvernområdet blir stadig viktigare. Fordi opplysningar i aukande grad kryssar landegrensene i samband med ulik tenesteutøving, blir òg personvernutfordringar og usemjer i større grad grenseoverskridande. Det krevst internasjonalt samarbeid både for å førebyggje og for å løyse slike usemjer. Regjeringa meiner det derfor er viktig at Noreg prioriterer å ta del i dei ulike internasjonale foruma der personvern er på saklista, og i så stor grad som mogleg freistar påverke utviklinga.

I kapittel 6 i rapporten frå Personvernkommisjonen er det gjort greie for ulike internasjonale regelsett og kva dei har å seie for personvernet. I meldinga blir det gjort greie for nokre viktige utviklingstrekk på

det internasjonale området etter at Personvernkommisjonen avslutta arbeidet sitt.

2.1.2 EUs personverndirektiv og europeisk personvernsamarbeid

EUs direktiv 95/46/EF (heretter omtala som personverndirektivet) vart vedteke i 1995 og er EØS-relevant og bindande for Noreg.

2.1.2.1 EU-direktiv som er viktige for norsk personvernregulering

Personverndirektivet er i all hovudsak gjennomført i norsk rett gjennom personopplysningslova frå 2000. I meldinga blir det vist til at viktige element i direktivet er prinsippet om ei uavhengig tilsynsstyremakt, krav til rettsleg grunnlag for behandling av personopplysningar, aktiv informasjonsplikt for den behandlingsansvarlege overfor dei registrerte, særlege rettar for dei registrerte ved behandling av personopplysningar i automatiserte avgjerdsprosessar og meldeplikt til tilsynsstyremakta ved behandling av personopplysningar. Det er likevel opna for store unntak, mange av dei tufta på skjønsvurderingar, frå dei fleste prinsippa som er nedfelte i direktivet.

Personverndirektivet er eit minimumsdirektiv. I mange av føresegnene ligg det dessutan eit stort og skjønsprega handlingsrom. Medlemsstatane kan gjere ei rad meir eller mindre vidfemnande unntak frå det som er hovudregelen i direktivet. I meldinga blir det peikt på at dette fører med seg at den ønskte harmoniseringa, som ligg bak direktivet, likevel ikkje blir heilt nådd. Dette er noko av årsaka til at EU-kommisjonen i lengre tid har arbeidd med ein revisjon av det gjeldande personverndirektivet. Revisjonen blir omtala i kapittel 3.2.3 i meldinga.

Jamvel om reglane i personopplysningslova i all hovudsak er ei gjennomføring av personverndirektivet, er nokre av reglane i lova likevel norske spesialreglar. Dette gjeld særleg reglane i personopplysningslova om kameraovervaking. I samband med revisjonen av personverndirektivet som er i gang, har EU-kommisjonen likevel gjort framlegg om at det nye regelverket skal innehalde reglar om kameraovervaking. Dessutan inneheld personopplysningsforskrifta nokre reglar som ikkje beint er å finne i direktivet. Dette er mellom anna spesialreglar om informasjonstryggleik, om fritak frå melde- og konsesjonsplikt, om kredittopplysningsverksemd og om innsynet arbeidsgivaren har i e-posten til tilsette.

Personopplysningslova og -forskrifta inneheld føresegner om korleis norske styremakter og behandlingsansvarlege skal te seg når dei overfører personopplysningar til tredjeland, og om tilhøvet til avgjerder EU-kommisjonen tek om personvernnivået i desse landa. Desse avgjerdene om personvernnivået i tredjeland er EØS-relevante, og Noreg har til no lagt avgjerdene frå EU-kommisjonen til grunn i saker som gjeld overføring av personopplysningar til desse landa. Personverndirektivet er generelt. Det gjeld derfor for all behandling av personopplysningar så framt det ikkje er gjort unntak. Det går fram av direktivet at landa kan fråvike prinsippa i direktivet dersom dette er nødvendig til dømes av omsyn til den nasjonale tryggleiken, for kriminalitetsførebygging eller for å ta vare på særlege økonomiske interesser for eit land. At det av slike grunnar er mogleg å fråvike prinsippa i direktivet, er det teke omsyn til i personopplysningslova.

Direktiv 2002/58/EF (kommunikasjonsverndirektivet) inneheld personvernføresegner som gjeld generelt for elektronisk kommunikasjon. Direktivet er implementert i lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon med forskrifter. Dessutan regulerer direktiv 2006/24/EF (datalagringsdirektivet) plikta ekomtilbydarane har til å lagre trafikk- og kommunikasjonsdata for kriminalitetsmotverkande føremål. Dette direktivet vart vedteke gjennomført i norsk rett i 2011, men reglane har enno ikkje teke til å gjelde.

2.1.2.2 Noregs deltaking i europeisk personvernsamarbeid

Det finst to samarbeidsforum på personvernområdet i EU. Dei blir omtala som Article 29 Data Protection Working Party (Artikkel 29-gruppa) og Article 31 Working Party (Artikkel 31-gruppa). Artikkel 29-gruppa er samarbeidsforum for tilsynsstyremaktene i medlemslanda, medan Artikkel 31-gruppa er ein komité på departementsnivå. Denne gruppa har avgjerdsmakt når personverndirektivet krev samtykke frå medlemslanda til ei gitt handling. Dette gjeld til dømes vedtak om personvernnivået i tredjeland. EFTA-landa er ikkje med i Artikkel 31-gruppa. Noreg, representert ved Datatilsynet, har likevel vore med i Artikkel 29-samarbeidet sidan 1996. Det følgjer av EØS-avtala at Noreg skal ha observatørstatus, men ikkje røysterett i denne arbeidsgruppa. Gruppa gir EU-kommisjonen råd i spørsmål om personvern og informasjonstryggleik og kjem saman seks gonger i året.

Noreg er fullverdig medlem av The Schengen Joint Supervisory Authority (JSA), et uavhengig kontrollorgan som er samansett av medlemer frå datatilsynsstyremakter i statar tilknytte Schengenavtala.

Working Party Police and Justice (WPPJ) har mandatet sitt frå Den europeiske konferansen for datatilsynsstyremakter og har jamlege møte. Oppgåva er å følgje med på utviklinga på politi- og justisområdet når det gjeld behandlinga av personopplysningar.

Berlin-gruppa arbeider med personvern innan elektronisk kommunikasjon i utvida forstand. Datatilsynet er fullverdig medlem av arbeidsgruppa, som har brei deltaking frå alle delar av verda.

Internasjonalt saksbehandlarmøte er eit årleg arrangement der Datatilsynet deltek for å få innspel om kva styremaktene i andre land er opptekne av, og for å utveksle røynsler.

Fordi Noreg ikkje er medlem av EU, er Datatilsynet særleg oppteke av å ha eit tett og forpliktande samarbeid med dei andre nordiske landa. For å halde dette samarbeidet ved like har dei nordiske datatilsynsstyremaktene organisert et nordisk møte ein gong i året for leiarane for dei nordiske datatilsynsstyremaktene.

Regjeringa meiner det er både bra og viktig at Datatilsynet prioriterer det internasjonale samarbeidet høgt.

2.1.2.3 Revisjon av EUs personvernregulering

EUs gjeldande personverndirektiv (95/46/EF) har vore, og er framleis, eit viktig regelsett. Likevel er det liten tvil om at direktivet er moge for revisjon. Det har vore ei rivande utvikling i åra sidan direktivet vart vedteke.

25. januar 2012 la EU-kommisjonen fram utkast til revidert personvernregelverk. Eit ønske om betre harmonisering av personvernregelverka i dei europeiske landa har stått sentralt i arbeidet med å førebu regelverksrevisjonen. Tydelegare plikter for dei behandlingsansvarlege og klårare rettar for dei registrerte står sentralt i revisjonen. Det er gjort framlegg om å fjerne den relativt vidfemnande meldeplikta som gjeld i dag, og det er føreslått ei ordning der behandlingsansvarlege som er etablerte i fleire medlemsstatar, skal kunne halde seg til personvernstyremakta i berre eitt av desse landa. Det er òg framlegg om å harmonisere reglane om sanksjonering av brot på personvernregelverket. Tanken med framlegga er å lette dei administrative byrdene for dei behandlingsansvarlege.

Når det gjeld rettar, har fokus særleg vore retta mot omgrepet «right to be forgotten», som inneber ein rett til å bli gløymd når personopplysningane ikkje lenger er nødvendige for innsamlingsføremålet. Ein rett til å ta med seg personopplysningar frå eitt sosialt nettverk til eit anna er òg eitt av framlegga som skal betre personvernet på nett. Det er dessutan gjort framlegg om strammare reglar for samtykke som skal danne grunnlag for behandling av personopplysningar. Eit samtykke må vere konkret, informert og eksplisitt. Samstundes er det gjort framlegg om at berre foreldre eller føresette kan samtykke på vegne av barn under 13 år som får tilbod om informasjonssamfunnstenester. Eit tydelegare fokus på personvernfremjande bruk av teknologi står sentralt i revisjonsarbeidet. Auka bruk av innebygd personvern, eller «privacy by design» som er det mest kjende omgrepet, inneber at IKT-løysingar blir utvikla med dei personvernvenlege alternativa som innebygde førsteval. Den som skal bruke systemet, må gjere eit aktivt val dersom han eller ho ønsker å nytte mindre personvernvenlege alternativ. Det er vidare framlegg om klarare reglar om bruk av personvernombod (data protection officer) og oppgåvene deira, og reglar om obligatoriske personvernkonsekvensutgreiingar og internkontrollsystem. I forlenginga av dette blir det òg gjort framlegg om ei sertifiseringsordning som skal dokumentere at den behandlingsansvarlege sikrar eit tilfredsstillande personvernnivå.

I håp om å leggje til rette for ei betre europeisk harmonisering av personvernretten er regelutkastet presentert som ei forordning. Ei forordning må gjennomførast av landa etter ordlyden. Medlemslanda har derfor lite rom for nasjonale tilpassingar dersom det blir vedteke ei forordning om vern av personopplysningar. I tillegg til ei forordning om behandling av personopplysningar generelt har EU-kommisjonen lagt fram utkast til eit direktiv om behandling av personopplysningar for kriminalitetsførebygging. Dette direktivutkastet er i all hovudsak ei direktivfesting av rammeavgjerd 2008/977/JHA om vern av personopplysningar som blir behandla i politi- og justissamarbeid i Europa. Rammeavgjerda gjeld ved utveksling av personopplysningar mellom dei samarbeidande landa. Direktivutkastet legg opp til at dei same reglane òg langt på veg skal gjelde for korleis politiet nasjonalt behandlar personopplysningar i samband med avdekking, gransking, oppklaring og straffeforfølging av strafflagde handlingar. Når lov 28. mai 2010 nr. 16 om behandling av personopplysningar i politiet (politiregisterlova) med forskrifter tek til å gjelde, gjennomfører ho langt på veg reglane i rammeavgjerda som gjeld korleis norsk politi skal behandle personopplysningar nasjonalt. Lova kjem til å leggje til rette for god ivaretaking av personvern i viktige delar av justissektoren. Slik direktivutkastet frå EU no ser ut, er det derfor ingen grunn til å tru at dette fører til store behov for endringar i det norske regelverket.

Regelframlegga er til behandling i Rådet og EU-parlamentet. Regjeringa er positiv til mange av dei prinsippa som ligg til grunn for regelframlegga frå EU. Dersom regelverket blir vedteke slik EU kommisjonen har gjort framlegg om, vil det bli nødvendig med endringar i det norske personvernregelverket. Fleire av prinsippa og framlegga frå EU blir nærmare omtala i meldinga.

2.1.3 OECDs retningsliner om personvern

2.1.3.1 OECDs retningsliner om personvern – innhald og korleis dei verkar inn på norsk personvernrett

OECD vedtok retningsliner for vern og utveksling av personopplysningar over landegrensene i 1980 (Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data). Desse retningslinene er ikkje rettsleg bindande for medlemsstatane. Dei har likevel vore viktige for utviklinga av personvernregelverk i ei rekkje land, særleg utanfor Europa. OECD er ein viktig arena for internasjonalt personvernsamarbeid ut over det europeiske. Det blir i meldinga vist til at det er nyttig å diskutere handteringa av aktuelle personvernutfordringar innanfor OECD, fordi det gir eit innsyn i korleis styremaktene i andre land vurderer ulike personvernspørsmål. Røynsla er uansett at hovudproblemstillingane og utfordringane er felles for dei fleste landa, endå om landa har litt ulik tilnærming til korleis ein bør handtere utfordringane.

For det norske personvernregelverket har OECDs retningsliner om personvern og overføring av personopplysningar over landegrensene dei seinare åra likevel hatt lite å seie konkret og direkte.

2.1.3.2 OECDs arbeid med personvern og Noregs deltaking i arbeidet

OECDs personvernarbeid er lagt til arbeidsgruppa for informasjonstrygging og personvern (Working Party on Information Security and Privacy – WPISP), som så er organisert under komiteen for IKT (Committee for Information, Computer and Communications Policy – ICCP). OECDs retningsliner for personvern og flyt av personopplysningar over landegrensene har eit klårt personvernfokus. Ivaretaking av personvernomsyn, kanskje særleg i den forstand at personopplysningar ikkje skal kome uvedkomande i hende, er viktig ut frå OECDs perspektiv om økonomisk vekst og utvikling.

I 2010 vart det, i høve 30-årsjubileet for OECDs personvernretningsliner, sett i gang eit arbeid med sikte på å revidere retningslinene. For dei OECD-landa som òg er EU-/EØS-medlemer, er det sentralt å sjå regelsettet i dei to organisasjonane i samanheng.

Noreg deltek med representantar på departementsnivå både i OECDs IKT-komité og i arbeidsgruppa for personvern og informasjonstryggleik (WPISP). Regjeringa erfarer at deltaking i OECD-arbeidet er til stor nytte.

2.1.4 Personvernkonvensjonen til Europarådet

Europarådskonvensjon 28. januar 1981 nr. 108 om personvern i samband med elektronisk databehandling av personopplysningar (personvernkonvensjonen) vart ratifisert av Noreg 20. februar 1984 og tok til å gjelde 1. oktober 1985. Så langt har 43 land ratifisert konvensjonen.

Føremålet med personvernkonvensjonen er å tryggje respekten for fridom og andre grunnleggjande rettar i samband med lagring og handtering av personopplysningar ved hjelp av elektronisk databehandling. Konvensjonen inneheld minimumsreglar, og dei ulike landa står fritt til å gi personvernrettar som går ut over det som følgjer av konvensjonen. Konvensjonen er gjennomført i norsk rett gjennom personopplysningslova. Personvernkonvensjonen er seinare følgd opp med ulike rekommandasjonar (tilrådingar) som gir utfyllande retningsliner for behandling av personopplysningar på nærmare avgrensa område. Det er oppretta ein konsultativ komité i samsvar med personvernkonvensjonen artikkel 18 (T-PD). Noreg stiller normalt med ein representant på dei årlege møta i komiteen.

Det er nyleg sett i gang ein prosess i Europarådet som skal modernisere personvernkonvensjonen. Eit viktig omsyn er å tryggje samsvar mellom personvernregelverket som er under utarbeiding i EU, og Europarådskonvensjonen.

2.1.5 Overføring av personopplysningar til utlandet – bruk av standardavtaler og Binding Corporate Rules

Personopplysningslova set krav som må vere oppfylte før ein behandlingsansvarleg som er etablert i Noreg, kan eksportere personopplysningar ut av landet, jf. lova §§ 29 og 30. Så lenge personopplysningane skal eksporterast til statar i EØS-området, er det ingen restriksjonar. Overføring av personopplysningar kan òg skje fritt til aktørar i tredjeland som EU-kommisjonen ved ei formell avgjerd har funne å ha eit tilfredsstillande vernenivå. Med mindre Noreg reserverer seg, gjeld avgjerdene kommisjonen tek på dette området òg for Noreg.

I alle andre tilfelle der den behandlingsansvarlege ønskjer å overføre personopplysningar til utlandet, må anten eitt eller fleire av unntaka i personopplysningslova § 30 første leddet vere oppfylte, eller Datatilsynet kan godkjenne overføringane som skal gjerast. Bruksområdet for dei nemnde unntaka er likevel nokså snevert, ifølgje Artikkel 29-gruppa. Den offisielle tilrådinga frå Datatilsynet er derfor at den behandlingsansvarlege anten nyttar standardkontraktane som EU-kommisjonen har laga for dette føremålet, eller at det blir utforma såkalla Binding Corporate Rules, ofte omtala som BCR. Sjå meldinga for ei nærare omtale av standardkontrakter og BCR, og om rolla til Datatilsynet i dette arbeidet.

2.1.6 Hovudpunkt kapittel

– Noreg skal vere ein relevant bidragsytar i internasjonalt personvernarbeid.
– Noreg vil arbeide for deltaking i eit eventuelt nytt europeisk datatilsyn og deltaking i avgjerdsprosessen i EU-kommisjonen der denne får kompetanse etter EØS-relevant personvernregelverk.
– Regjeringa vil arbeide for god nasjonal samordning av Noregs internasjonale personvernarbeid.

2.2 Komiteens merknader

Komiteen viser til at det någjeldende EU-direktiv (95/46/EF) er under revisjon og skal erstattes av en forordning som vil få betydelig innvirkning på EØS-området. Det er uklart når forslaget ferdigbehandles i EU, men Norge må arbeide for deltagelse i beslutningsprosessen.

Selv om personverndirektivet er bindende for Norge, er det likevel et nasjonalt handlingsrom, som komiteen forventer blir utnyttet hvis nasjonale behov tilsier strengere personvern.

Komiteen har merket seg Norges brede deltakelse, i første rekke gjennom Datatilsynet i internasjonalt personvernarbeid, og legger vekt på at Norge gjør sin innflytelse gjeldende, særlig overfor EU-systemet.

Komiteens medlemmer fra Fremskrittspartiet, Høyre og Kristelig Folkeparti mener det er nødvendig å innføre «Privacy by Design» i alle offentlige IKT-prosjekter.

Disse medlemmer mener det er skuffende at regjeringen i denne meldingen ikke signaliserer at man vil ta opp forholdene rundt den svenske FRA-loven (Lag om ändring i lagen om försvarsunderrättelseverksamhet), en lov som gir en sivil etat, under det svenske forsvarsdepartementet, rett til å bedrive kommunikasjonsetterretningsvirksomhet på kabelbåren trafikk som passerer svenske grenser, hvilket altså innbefatter telefoni og en betydelig andel av internettrafikken. Disse medlemmer viser til at Datatilsynet og Post- og teletilsynet uttrykte sterk bekymring da denne loven i 2011 ble utvidet til å gi tilgang til kommunikasjonsetterretninger for de særskilte politiorganene Rikskriminalpolisen og Säkerhetspolisen. Selv om den svenske regjeringen i svar på skriftlig spørsmål fra stortingsrepresentant Hans Frode Asmyhr gjennom Nordisk råd, jf. E3/2012 (http://www.norden.org/da/nordisk-raad/sager/spoergsmaal-og-svar/2012/e-3-2012), betoner at den formen for informasjonsinnhenting som er hjemlet i FRA-loven, innebærer en domstols godkjennelse, åpner denne muligheten for å drive etterretningsinnhenting for utvidede fullmakter til at sivile svenske myndigheter kan overvåke 80 pst. av data- og teletrafikk inn og ut av Norge. Disse medlemmer er urolige for at de begrensninger som ligger i denne loven når det gjelder kontroll av borgere, ikke innbefatter andre enn svenske borgere.

På denne bakgrunn fremmer disse medlemmer følgende forslag:

«Stortinget ber regjeringen gjennomgå implikasjonene av utvidelsene av den svenske FRA-loven og fremme en sak til Stortinget om hvordan man kan sikre at innbyggere i Norge får bedre beskyttelse i sin tele- og datakommunikasjon.»

3. Proporsjonalitet og avveging av ulike samfunnsomsyn

3.1 Sammendrag

3.1.1 Generelt om vurderinga av behandling av personopplysningar i det offentlege

Det blir i meldinga peikt på at omsynet til personvernet må vurderast opp mot andre viktige samfunnsomsyn og interesser i ei såkalla proporsjonalitetsvurdering. Dette inneber ofte vanskelege avvegingar mellom omsyn som kvar for seg er viktige. Avveginga krev grundige vurderingar frå område til område. Vektige motomsyn kan for eksempel vere meir effektiv offentleg tenesteyting, kontrollføremål, kriminalitetsførebygging, ytringsfridom og tilrettelegging for gode helse- og omsorgstenester. I ei avveging er det sjeldan eit spørsmål om berre to alternative løysingar. Vidare kan ein ofte setje i verk ulike tiltak for å minske ulemper og utnytte fordelar ved dei alternative løysingane.

Noreg er eit velferdssamfunn, og det offentlege har eit stort ansvar for å drive tenesteyting til folket.

Det er nødvendig for forvaltninga å kunne samle inn og registrere informasjon om innbyggjarane for å kunne fastsetje rettane og pliktene deira. Når lovgivaren fastset ein rett til å behandle personopplysningar, er det viktig å synleggjere proporsjonalitetsvurderingane som ligg bak, slik at ein kan prøve premissane for vurderinga lovgivaren har gjort.

3.1.2 Helse- og omsorgstenester

Ved yting av helse- og omsorgstenester kan det vere vanskeleg å avgjere på førehand kva opplysningar som er nødvendige. Då treng ein ofte å hente inn mykje informasjon om einskildpersonen for å sikre han eller ho best moglege tenester. Relevante og nødvendige opplysningar om pasienten og helsehjelpa skal skrivast i journal for kvar einskild pasient, jf. helsepersonellova kapittel 8.

Informasjonsforvaltinga skal gjere sitt til å ta vare på grunnleggjande pasienttryggleik.

Det blir i meldinga peikt på at det er ei utfordring at dokumentasjonen inneheld store mengder sensi-

tive personopplysningar. Kjernen i utfordringa er å vege to pasientinteresser mot einannan – at opplysningane er tilgjengelege for helsepersonellet, må vegast mot at pasienten ønskjer så stor konfidensialitet som råd. Godt personvern er ein viktig del av pasienttryggleiken. Samfunnsutviklinga, med auka bruk av teknologi, stiller stadig større krav til effektivitet og omstillingar i helse- og omsorgstenesta. Elektroniske system inneber ofte ei større samling av opplysningar med auka høve til å stille saman og spreie personopplysningar enn det som var mogleg med tidlegare papirjournalar. Samstundes opnar den tekniske utviklinga òg for betre ivaretaking av personvernet. I meldinga blir det peikt på at det kan hende er viktigast at det er mogleg å logge oppslag for å førebyggje såkalla «snoking», effektive system for tilgangskontroll og at det er mogleg å kryptere opplysningar.

Hovudtyngda av opplysningane som blir behandla i helse- og omsorgstenesta, er underlagd teieplikt etter helsepersonellova og forvaltningslova.

Sjølvråderetten og retten til konfidensialitet har fått stor vekt i ordskifta dei siste tiåra. Desse omsyna må like fullt vegast mot behovet for å ha den kunnskapen som er nødvendig for å kunne kontrollere effekten av behandlinga, og eventuelt for å påvise svake punkt i pasienttryggleiken og mogelege skilnader sjukehusa imellom.

Regjeringa meiner at det ikkje er nokon motsetnad mellom personvern og pasientinteresser.

Utgreiinga frå Personvernkommisjonen legg vekt på at helse- og omsorgssektoren står overfor personvernutfordringar. Regjeringa er samd i denne vurderinga. Desse utfordringane er bakgrunnen for at det gjennom mange år har gått føre seg eit systematisk arbeid for å styrkje personvernet i helse- og omsorgssektoren, både organisatorisk, juridisk og teknologisk. Regjeringa vil halde fram arbeidet med å styrkje personvernet mellom anna ved å leggje til rette for loggføring av interne oppslag i større register. Sjå nærmare omtale i kapittel 9.6.3 i meldinga.

For å ta vare på personvernet bør ein gjennomføre tiltak som hindrar eller motverkar uautorisert behandling og spreiing av opplysningar. Dette kan vere reglar om teieplikt, logging av oppslag i journalar og tilgangskontroll. Ein bør leggje til rette for «innebygd» personvern i dei ulike systema som blir nytta, og staten bør som innkjøpar spørje etter gode system. Vidare er informasjon om rettar og plikter for helsepersonell og brukarar eit viktig tiltak.

3.1.3 Kriminalitetsførebygging

Det blir i meldinga peikt på at det er viktig å leggje til rette for at politiet er i stand til å motverke kriminalitet. Omsynet til personvernet må likevel tryggjast på dette området, og i somme tilfelle veg personvernomsyn tyngre enn omsynet til kriminalitetsførebygging.

I avveginga av dei to omsyna spelar det mellom anna inn kor alvorleg kriminalitet det er tale om å hindre. Strafferamma for handlinga som blir granska, ligg ofte til grunn i vurderingar av kva opplysningar politiet kan hente inn. Vidare vil ein leggje vekt på kor sensitive opplysningar det er tale om, og kor stor den samla integritetskrenkinga for den registrerte er.

Førebygging av kriminalitet står ikkje alltid i motsetnad til personvernet. For eksempel er det i tråd med begge desse omsyna å hindre at overgrepsbilete blir tilgjengelege på nett, eller å førebyggje identitetstjuveri.

Regjeringa meiner datainnsamling i samband med kriminalitetsførebygging er nødvendig og ønskjeleg for å førebyggje, hindre og granske kriminalitet. Det er likevel viktig at ein tryggjar personvernet i så stor grad som råd, og at det blir gjennomført grundige utgreiingar av kvifor ein treng tilgang til personopplysningane. Dataminimalitet er eit mål. Tiltak som tek vare på personvernet, kan vere reglar om teieplikt og krav til trygging av register (logging, kryptering og så vidare).

3.1.4 Utdanning

Personopplysningar blir nytta til mange ulike føremål i utdanningssektoren og i barnehagane. Ein fellesnemnar er at personopplysningane blir nytta til å tilby tenester av tilfredsstillande kvalitet. For skoleeigarar spesielt, men også for barnehageeigarar, kan bruk av personopplysningar vere nødvendig for å oppfylle lovpålagte oppgåver. Det blir i meldinga peikt på at det er viktig at det ikkje blir behandla meir personopplysningar enn nødvendig, samstundes er det til dømes avgjerande at ei sak blir så godt opplyst som mogleg før vedtak blir fatta.

Både kvar einskild skule og kvar einskild barnehage behandlar personopplysningar for å kunne gi elevar og barn i barnehage tilfredsstillande oppfølging. Universitet og høgskular har òg oversikt over studentane og lærarane til bruk i administrasjonen. Slike register er etter personopplysningsforskrifta unntekne frå konsesjonsplikta. Unntaksheimelen viser at det alt er gjort ei vurdering av at dette er nødvendig behandling i desse sektorane, og at behandlingane ikkje fører med seg store personvernkrenkingar.

Det blir i meldinga gjort greie for ulike meldingar frå regjeringa:

- St.meld. nr. 41 (2008–2009) Kvalitet i barnehagen
- St.meld. nr. 44 (2008–2009) Utdanningslinja
- Meld. St. 22 (2010–2011) Motivasjon – Mestring – Muligheter, Ungdomstrinnet
- Meld. St. 18 (2010–2011) Læring og Fellesskap.

Overføring av personopplysningar mellom barnehage og skule og skular imellom inneber spreiing av personopplysningar. Utvekslinga av informasjon er som hovudregel basert på samtykke frå dei føresette. På denne måten held ein kontroll med eigne personopplysningar samstundes som barnehagen/skulen får det nødvendige kunnskapsgrunnlaget for å leggje kvardagen til rette for barnet/eleven. Regjeringa legg til grunn at det er nødvendig å behandle personopplysningar i denne samanhengen. Personvernet til den registrerte blir teke vare på gjennom bruk av samtykke. Regjeringa legg vidare til grunn at behandling av personopplysningar som hovudregel er nødvendig for å få teneste av ønska kvalitet i utdanningssektoren.

3.1.5 Behandling av personopplysningar i Arbeids- og velferdsetaten (Nav)

Tilsette i Arbeids- og velferdsetaten behandlar mange sensitive personopplysningar og opplysningar som kjem inn under teieplikta. Samtidig er tilgang til personopplysningar i Arbeids- og velferdsetaten avgjerande for å løyse dei lovpålagde oppgåvene til etaten. Teieplikta for tilsette i Arbeids- og velferdsetaten er streng. Dette er noko etaten er særs merksam på. Betydelege ressursar blir nytta for å ta vare på personvernet til brukarane.

Behandling av ei stor mengd personopplysningar er forpliktande. Etaten må balansere omsynet til effektiv sakshandsaming, korrekte vedtak og nødvendig kontroll mot den retten kvar einskild har til personvern.

Moderne IKT-system og saksbehandlingsverktøy er avgjerande for effektiv verksemd og kvalitativt god forvaltning av tenestene og stønadene etaten yter. Teknologien gjer det mogleg å styrkje personvernet, men fører òg med seg enkelte farar. Systema inneber mellom anna at personopplysningar om svært mange brukarar er samla i sentrale databasar. Dette krev gode system og rutinar for tilgangskontroll, innsynslogging og informasjonssikring. Datatilsynet har ved kontrollar både i sentrale og lokale einingar i 2007, 2010 og 2012, funne brot på krava til fortruleg behandling i personopplysningslova. Arbeids- og velferdsetaten har dei siste åra òg fått kritikk frå Riksrevisjonen.

Det blir i meldinga vist til at Arbeids- og velferdsetaten arbeider planfast og langsiktig for å lukke avvik som blir påpeikte av Datatilsynet og Riksrevisjonen.

Til dels kompliserte regelverk og produksjonsprosessar og ein kompleks organisasjon gjer det utfordrande å leggje til rette for ein føremålstenleg IKT-struktur som oppfyller alle krava i personopplysningslova. Bruk av mange gamle og fragmenterte IKT-system frå tidlegare etatar gjer utfordringane endå større. Programmet for IKT-modernisering vil i perioden 2013–2019 etablere ei ny plattform for framtidige saksbehandlingsløysingar på stønadsområda til Arbeids- og velferdsetaten. I kravspesifikasjonen til nye systemløysingar er det sett absolutte krav til personvern og informasjonstryggleik.

IKT-moderniseringa inneber mellom anna nye løysingar for administrasjon og kontroll av tilgangar og loggar.

Planane for IKT-moderniseringa har eit tidsperspektiv på seks år. Det er derfor nødvendig at etaten i mellomtida gjennomfører kortsiktige tiltak for å redusere risiko. Dette arbeidet er etaten godt i gang med.

Det er eit mål for Arbeids- og velferdsetaten at den tilgangen dei tilsette har til personopplysningar, ikkje skal overskride det kvar einskild har sakleg behov for.

Arbeids- og velferdsetaten har utarbeidd og operasjonalisert sentrale, leiande dokument for personvern og informasjonssikring.

I 2011 innførte etaten elektronisk behandling av dokument og elektronisk arkivering på viktige saksområde.

Trass i at etaten behandlar fleire millionar saker årleg, får Arbeids- og velferdsetaten få klagar over misbruk av personopplysningar. Etaten har arbeidd målretta med haldningsskapande tiltak knytte til teieplikt og personvern. I rapportane Datatilsynet har skrive frå tilsyn med Arbeids- og velferdsetaten, har tilsynet lagt til grunn at det er høgt medvit om personvern i etaten, at etatsleiinga tek personvernutfordringane på alvor, og at etaten arbeider godt med problema.

I meldinga blir det lista krava Arbeids- og velferdsdirektoratet har stilt til behandling av personopplysningar i Arbeids- og velferdsetaten.

Regjeringa ser det slik at Arbeids- og velferdsetaten er i ein god prosess med å sikre at personopplysningar blir behandla på ein trygg måte. Etaten har visse utfordringar, særleg når det gjeld tilpassing av tilgangskontrollar og oppfølging av loggar. Etaten søkjer ein god balanse mellom å løyse forvaltningsoppgåvene sine med eksisterande teknologi og å fylle krava til personvern og informasjonstryggleik. Regjeringa forventar betring av informasjonstryggleiken og personvernet på stønadsområda etter kvart som etaten får moderne IKT-støtte. Det er viktig at etaten i perioden fram til dei nye systema kjem på plass, held fram med arbeidet med kortsiktige risikoreduserande tiltak.

3.1.6 Ulike offentlege kontrollføremål

Meir og meir av rettshandhevinga i samfunnet blir lagd til offentleg forvaltning.

Det vernet som gjeld for ein som er sikta i ei straffesak, gjeld ikkje automatisk i ei forvaltningssak. Då må ein ta vare på rettsvern- og personvernomsyn gjennom allmenne krav til mellom anna legalitet og god samanheng mellom opplysningane og bruken.

3.1.6.1 Avveging mellom behovet for kontroll og rettsvern

Norsk rettstradisjon byggjer på stor tillit mellom innbyggjarane og staten.

Det er særleg to omsyn som gjer seg gjeldande i samband med offentleg kontroll overfor einskildpersonar, og det er legalitetsprinsippet og det allmenne prinsippet om forholdsmessigheit, jf. EMK artikkel 8. Prinsippa set grenser for kva tiltak staten lovleg kan setje i verk overfor den einskilde.

Forholdsmessigheitsprinsippet krev at eit inngrep i den private sfæren må stå i eit rimeleg tilhøve til dei interessene samfunnet har i å gjennomføre tiltaket. Det må med andre ord skje ei avveging av interesser. Det er eit vilkår at tiltaket uansett ikkje skal vere meir inngripande enn det som er nødvendig for å ta hand om samfunnsinteressene.

Legalitetsprinsippet krev at alle tiltak staten set i verk, og som utgjer inngrep i den private sfæren til den einskilde, skal ha eit rettsleg grunnlag. Legalitetsprinsippet er relativt, slik at kravet til kor sterkt og klårt det rettslege grunnlaget er, blir tilpassa etter kor inngripande tiltaket er.

Når ein skal vurdere kor inngripande eit konkret tiltak er, må ein sjå på om tiltaket er frivillig eller blir påført den einskilde med tvang. Offentlege kontrolltiltak blir ofte gjennomførte utan samtykke frå innbyggjarane, og manglande medverknad kan i somme tilfelle straffast.

Det har vidare noko å seie om tiltaket kan krenkje den fysiske integriteten til den einskilde. Dette er typisk tilfelle når det skal gjerast kroppsvisitering eller i heimen til ein person.

Tiltak som fører med seg behandling av sensitive personopplysningar, er gjennomgåande meir inngripande enn tiltak som berre fører med seg behandling av ikkje-sensitive opplysningar. Føremålet med offentlege kontrolltiltak er ofte å sikre etterleving av regelverket. Dette kan føre med seg at det blir avdekt strafflagde handlingar. Opplysningar om at nokon er mistenkt for ei strafflagd handling, er opplysningar som er rekna for å vere sensitive. Vidare vil kontrollar, i tilfelle der dette er relevant for kontrollføremålet, kunne innebere at det blir innhenta sensitive opplysningar.

Det har òg noko å seie kor vidt behandlinga av personopplysningar femner, både med tanke på talet på registrerte, mengda av opplysningar om den einskilde og kor lenge behandlinga skal halde fram.

Endeleg har det noko å seie om tiltaket fører med seg spreiing av eksisterande personopplysningar. Dersom kontrollorganet berre behandlar opplysningar det alt sit inne med, er det mindre inngripande enn dersom organet hentar inn nye opplysningar for kontrollføremålet.

3.1.6.2 Vurderinga av forholdsmessigheit

Offentlege kontrolltiltak kan føre med seg store inngrep i personverninteressene til den einskilde. Tiltaka blir i stor grad gjennomførte med tvang og fører ofte med seg behandling av sensitive personopplysningar. Offentlege kontrolltiltak kan berre setjast i verk dersom det ligg føre tungtvegande interesser som krev at kontrollen skal gjennomførast. EMK artikkel 8 set grenser for kva kontrolltiltak lovgivaren kan vedta. Det blir i meldinga vist til at i praksis er denne avgrensinga likevel mest av teoretisk interesse, fordi opplistinga femner særs vidt.

Ulike samfunnsinteresser har ulik vekt.

Det er krevjande å vege samfunnsinteressa i eit kontrolltiltak mot personvernomsyn. For det første er personvernet ei ideell interesse som ein ikkje lett kan måle og vege. Vidare er det slik at personverninteressene først og fremst er individuelle, medan samfunnsinteressa er kollektiv.

Samtykke frå den registrerte er ofte rekna for å vere det føretrekte rettslege grunnlaget ved behandling av personopplysningar. Når det gjeld offentlege kontrollføremål, er likevel samtykke lite eigna. For det første er styrketilhøvet mellom stat og innbyggjar ofte så skeivt at ein kan spørje om samtykket verkeleg er frivillig. For det andre veg samfunnsomsyna ofte så tungt at sjølvråderetten til den registrerte uansett må setjast til side.

3.1.6.3 Innhenting av opplysningar frå parten sjølv

Dersom den einskilde sjølv får høve til å leggje fram personopplysningane som er nødvendige for å klårgjere ei forvaltningssak, får vedkomande betre kontroll med eigne opplysningar. Dette tek normalt vare på grunnleggjande personvernomsyn, så framt manglande innlevering av opplysningar ikkje fører til tvangstiltak eller mistanke om uærlegdom.

Ved innhenting av opplysningar for offentleg kontroll, er det likevel gode grunnar til heilt eller delvis å byte ut eller supplere opplysningane frå parten sjølv med opplysningar som blir henta frå andre kjelder. Personvernomsyna må då først og fremst tryggjast gjennom å gi den registrerte informasjon om innhentinga og høve til motsegn.

3.1.7 Forsking

Det blir i meldinga vist til at ivaretaking av personvernomsyn er eit grunnleggjande forskingsetisk

prinsipp. Bruk av personopplysningar i forsking er tydeleg regulert, og forskarane må rette seg etter fleire ulike regelsett og godkjenningsinstansar.

Den generelle teknologiske utviklinga utfordrar personvernet også innan forskinga.

Det går fram av meldinga at det er eit mål i forskingspolitikken å leggje til rette for open tilgang til offentleg finansierte forskingsdata. I dette arbeidet må ein òg ta vare på personvernaspektet, for eksempel gjennom reglar om tilgang og vilkår for bruk av personopplysningar.

TILHØVET TIL PERSONOPPLYSNINGSLOVA

Forskingsprosjekt som inneber behandling av personopplysningar, fell inn under personopplysningslova og er som hovudregel meldepliktige til Datatilsynet, så framt prosjekta er godkjende av personvernombodet for forsking i verksemda. Helsefagleg forsking blir som hovudregel regulert av helseforskingslova. Prosjekta må som utgangspunkt leggjast fram for dei regionale komiteane for medisinsk og helsefagleg forskingsetikk (REK), men dei må òg vurderast mot helseregisterlova.

Norsk samfunnsvitskapleg datateneste (NSD) er personvernombod for forskings- og studentprosjekt som blir gjennomførte ved universitet, statlege høgskular, vitskaplege og private høgskular, ei rad helseføretak og andre forskingsinstitusjonar.

For prosjekt som blir vurderte som konsesjonspliktige, sender personvernombodet søknad til Datatilsynet på vegne av forskaren eller studenten. Prosjektet kan ikkje setjast i gang før Datatilsynet har gitt konsesjon (førehandsgodkjenning). Når søknader om konsesjon skal avgjerast, legg Datatilsynet mellom anna vekt på om behandlinga av personopplysningane kan medføre ulemper for den einskilde.

KRAV TIL SAMTYKKE

Som hovudregel skal forskingsprosjekt som inkluderer personar, berre setjast i gang etter eit frivillig, uttrykkeleg og informert samtykke frå deltakarane. Informantane har til kvar tid rett til å avbryte deltakinga si, utan at dette får negative konsekvensar for dei.

Behovet for lettfatteleg informasjon til deltakarane er særleg stort viss forskinga inneber ei eller anna form for risiko for deltakarane.

Kravet om samtykke skal førebyggje krenkingar av personleg integritet. Det er utarbeidd eigne retningsliner for korleis ein på visse vilkår kan drive forsking som inkluderer menneske med redusert eller manglande samtykkekompetanse. Innhenting av opplysningar til bruk i forsking kan òg gjerast ved fritak frå teieplikta i § 13 d i forvaltningslova.

KONFIDENSIALITET

Tillit, lojalitet og fortrulegskap er grunnelement i det ansvaret forskaren har for den det blir forska på. Fortrulegskap inneber at tilgangen til informasjon blir avgrensa til dei som er autoriserte for tilgang. Fortrulegskapen blir normalt skjerpt etter kor sensitiv informasjonen er, og også etter kor utsett den det blir forska på, er.

Opplysningar om personar som tek del i forskingsprosjekt, skal behandlast «forsvarleg», det vil seie at ein skal handtere opplysningane i samsvar med lover og reglar, eventuelt òg i samsvar med lovnader som er gitt til den opplysningane gjeld. Metodekravet om etterprøveleg forsking inneber at ein ikkje alltid kan sikre fortrulegskap ved historiske og personretta studiar. For einskildindividet kan det liggje eit vern i at forskaren anonymiserer eller avidentifiserer innsamla data. Samstundes fører dette i dei fleste tilfelle til at kontrollen av forskingsprosjektet og av om resultata er gyldige, blir vanskelegare, og kan tene like mykje til vern av forskaren som av den som har gitt forskaren informasjon.

Reint metodisk kan det somme tider vere nødvendig å fire på andre vitskaplege standardar for å sikre fortrulegskapen. Dette gjeld ikkje minst det vitskaplege idealet om at ein skal kunne etterprøve forskinga.

3.1.8 Arbeidsliv

Personvern i arbeidslivet handlar om ei interesseavveging mellom behovet arbeidsgivaren har for å kontrollere kva som går føre seg i verksemda, og behovet arbeidstakaren har for vern av personleg integritet og personlege opplysningar. Det rettslege utgangspunktet er den ulovfesta retten arbeidsgivaren har til å organisere, leie, kontrollere og fordele arbeidet – den såkalla styringsretten til arbeidsgivaren. Styringsretten er avgrensa av lov, tariffavtaler og individuelle avtaler og rettspraksis.

Eksempel på kontrolltiltak er kameraovervaking i arbeidslokala, overvaking av telefonbruk, kontroll av e-post eller kva internettsider arbeidstakaren nyttar, lokalisering og sporing gjennom til dømes mobiltelefonar eller GPS, tilgangskontroll som viser kvar den tilsette er, bruk av «hemmeleg kunde» eller ransaking/kroppsvisitering.

Dei allmenne vilkåra som må vere oppfylte for at eit kontrolltiltak skal vere lovleg, knyter seg til omgrepa saklegheit og proporsjonalitet, som er velkjende arbeidsrettslege normer. Både teknologi, økonomi, tryggleik, arbeidsmiljø og helsemessige tilhøve kan gi sakleg grunn for kontrolltiltak.

Saklegheitskravet har to hovudelement. For det eine må ein ha eit sakleg føremål med kontrolltiltaket som er forankra i sjølve verksemda. Det blir òg kravd at tiltaket er eigna til å avdekkje det ein vil kontrol-

lere, det vil seie at det er føremålstenleg (testresultata må vere pålitelege, elles er dei ikkje eigna). For det andre gjeld kravet om sakleg grunn gjennom heile behandlingstida.

Momenta i saklegheitsvurderinga er òg relevante i ei vurdering av om eit isolert sett sakleg kontrolltiltak fører med seg urimelege ulemper for arbeidstakarane.

Ved vurderinga av rimeleg samsvar må ein òg sjå på summen av kontrolltiltak i verksemda.

Dei arbeidsrettslege reglane inneheld den same norma for personvern som personopplysningslova byggjer på, men dei to regelsetta bruker ulike omgrep.

Alle typar helsekontrollar, både kliniske og biologiske, må i utgangspunktet reknast som inngrep i den personlege integriteten til den einskilde arbeidstakaren. Slik kontroll er derfor avgrensa til det som er strengt nødvendig ut frå omsynet til verksemda. Helseundersøking av dei tilsette krev heimel i lov og er berre lovleg dersom stillinga inneber ein særleg risiko, eller når det er nødvendig for å verne liv eller helse. Kravet om at undersøkinga må vere nødvendig, skal tolkast strengt. Faren må vere alvorleg og stå fram som konkret, nærliggjande og sannsynleg.

Ei av dei vanlegaste formene for kontrolltiltak, som det òg er mange spørsmål rundt, er høvet arbeidsgivaren har til innsyn i e-postkassa til arbeidstakarane. Dette spørsmålet er særleg regulert i personopplysningsforskrifta kapittel 9. Vilkåra for innsyn i postkassa til arbeidstakarane er:

«når det er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten» eller «ved begrunnet mistanke om at arbeidstakers bruk av e-postkassen medfører grovt brudd på de plikter som følger av arbeidsforholdet, eller kan gi grunnlag for oppsigelse eller avskjed».

Men saksbehandlingsreglane om informasjon og drøfting i arbeidsmiljølova skal òg leggjast til grunn ved dette kontrolltiltaket.

3.1.9 Bokføringsplikt i handel og finans

Bokføringsplikta er regulert i bokføringslova og bokføringsforskrifta og har som føremål å sikre tilfredsstillande registrering og dokumentasjon av dei økonomiske aktivitetane til bokføringspliktige.

For å vere i samsvar med føremålet må bokføringa oppfylle dei grunnleggjande bokføringsprinsippa som går fram i bokføringslova § 4. Dette inneber m.a. at bokføringa må vere fullstendig, og at bokførte opplysningar må vere dokumenterte på ein måte som syner at dei er rettkomne. Vidare er det ein føresetnad for etterkontroll at det er teke vare på dokumentasjonen.

Reglane fører i mange tilfelle til at personopplysningar blir behandla.

Etter bokføringslova § 13 gjeld det krav til lagring av pliktig rekneskapsrapportering, spesifikasjonar av pliktig rekneskapsrapportering, dokumentasjon av bokførte opplysningar m.m. og nummererte brev frå revisor i ti år. Avtaler, brevskifte med viktige tilleggsopplysningar, utgåande pakksetlar og prisoversikter som skal utarbeidast i samsvar med lov eller forskrift, skal lagrast i tre år og seks månader.

Lagring av personopplysningar i det omfanget bokføringsregelverket legg opp til, kan utfordre personvernet. Informasjonen må derfor vere underlagd nødvendig sikring. Samstundes er det viktig å gjere gode analysar av personvernkonsekvensar når lagringsplikt blir vedteken eller endra, slik at lagring av kjøpsdetaljar blir avgrensa til eit nødvendig minimum.

3.1.10 Hovudpunkt kapittel

- Avveging av ulike interesser og proporsjonalitetsvurderingar skal synleggjerast, slik at dei kan etterprøvast og diskuterast.
- Ein kan berre behandle personopplysningar til offentlege kontrollføremål når det er nødvendig. Det skal vurderast tiltak som kan minske eventuelle ulemper for personvernet. Aktuelle tiltak kan vere tilgangsstyring og innsynslogging, kryptering, informasjonsavgrensing og sikring av gode rutinar i kvart einskilt organ.

3.2 Komiteens merknader

Komiteen har notert seg regjeringens omtale av proporsjonalitetsprinsippet, som skal hjelpe til med å finne en forsvarlig balanse mellom den enkeltes personvern og det offentliges interesse i å kjenne til en del fakta om individene, med tanke på administrasjon og kontroll, men også sikring av rettigheter, likebehandling og forskning. Komiteen mener at det er vesentlig for å finne frem til balanserte løsninger, at man har klart for seg hvilke momenter som hører til en avveining der individinteresse kan stå mot samfunnsinteresse. Komiteen vil likeledes understreke at en prinsipiell tilnærming kan gjøre det lettere å etterprøve og eventuelt justere praksis.

Komiteens medlemmer fra Fremskrittspartiet, Høyre og Kristelig Folkeparti vil peke på at Personvernmeldingens nokså ensidige fokus på personvernets stilling som følge av de tekniske muligheter for lagring, gjenfinning og spredning av personopplysninger, lett kan få en til å glemme at det inngår et proporsjonalitetsprinsipp i en overordnet lære om hvilke grenser en rettsstat må respektere uansett nødvendighetsargumentasjon. Dypest sett: hvilken kjerne av privatliv som må være

i behold uten statlige inngrep, og som ikke kan «avveies bort».

Disse medlemmer mener det er et foruroligende trekk ved meldingen at behovet for et slikt kjerneområde for individenes integritet, ikke omtales uttrykkelig.

Disse medlemmer viser til at mot slutten av 1700-tallet la det tyske rettssystem grunnlaget for det proporsjonalitetsprinsippet som i dag eksisterer i europeisk rett – og dermed også for det nødvendighetskriterium som er sentralt i problemstillingen. Proporsjonalitetsprinsippet er i økende grad bærende for EU-retten, og har dermed også konsekvenser for anvendelsen av persondatadirektivet. I Norge er dette prinsippet omtalt som et «forholdsmessighetsprinsipp».

Disse medlemmer understreker at EU-rettens forholdsmessighetsprinsipp, som danner bakgrunnen for kravet til nødvendighet, og som finnes i Personverndirektivets (Direktiv 95/46/EF av 24. oktober 1995) artikkel 7 og 8, også omhandler grunnlaget for behandling av opplysninger og de enkelte behandlingsgrunnlag. Prinsippet danner dermed grunnlag for de krav vi må stille til nødvendigheten av å behandle opplysninger etter den norske personopplysningsloven. Ved vedtak av den varslede forordning, vil EUs ordlyd være direkte bindende for norsk rett og må fortolkes direkte av norske rettsbrukere, forvaltning og domstoler.

Disse medlemmer minner om at en grunnleggende tanke bak forholdsmessighetsprinsippet er ideen om at det alltid skal være et rimelig forhold mellom mål og midler. Det stilles en rekke krav på veien for å anse prinsippet som tilfredsstilt. For det første må de inngrep som iverksettes, tilfredsstille kravet til egnethet. Det er for å sikre at de inngrep som gjøres for å nå de oppgitte samfunnsmessige mål, tilsvarer deres betydning. Det er ingen grunn til at noen skal tåle dårligere personvern uten at noe vesentlig oppnås. Det stilles altså et krav om særskilt vurdering av om inngrepet er avpasset i forhold til formålets betydning. I EU-domstolens praksis etter årtusenskiftet har man gått over fra å benytte kriteriet hensiktsmessig til en drøftelse av virkemiddelets egnethet.

Disse medlemmer vil hevde at kravet til en avveiningsrimelighet i sin kjerne gjennomgående er formulert slik av Domstolen:

«Hvis det er mulighet for å velge mellom flere egnede tiltak, skal det minst inngripende middel velges, og inngrepet må til slutt ikke fremstå uforholdsmessig i forholdet til de tilsiktede mål».

Disse medlemmer uttrykker at også kravet til nødvendighet er et integrert prinsipp for behandlingsgrunnlagene i personopplysningsloven. Kravet om nødvendighet er ett av tre underprinsipper for å oppfylle et mer overordnet forholdsmessighetskrav.

Disse medlemmer viser til at personopplysning og behandling er grunnleggende begreper i personopplysningsloven (pol.), og brukes i en stor del av lovens bestemmelser. Begge begrepene avgrenses meget romslig. Den brede definisjon av begrepene medfører at stort sett alle opplysninger som kan henføres til en enkeltperson, og de fleste tenkelige former for behandling, faller inn under lovens begreper. Dette er ikke det samme som at alle behandlingsformer er like inngripende overfor den registrerte.

Disse medlemmer vil minne om at spredning av opplysninger er en særlig inngripende form for behandling, gjenbruk til utvidede formål likeså. Differensiering ut fra de enkelte behandlingsformene og graden av inngrep påvirker også det kravet som bør stilles til nødvendighet. Det skal stilles større krav til nødvendigheten av en samkjøring eller en videreformidling enn til nødvendigheten av at det skjer en registrering og lagring med henblikk på den behandlingsansvarliges egen bruk.

Disse medlemmer mener det samme også vil gjelde for karakteren av personopplysningene. Nødvendighetskriteriet må stilles strengere for følsomme opplysninger enn for mer alminnelige opplysninger. Det behøver ikke bety at grensen settes spesielt lavt for de sistnevnte opplysninger, eller at man skal ta lett på registrering der dette skjer til den behandlingsansvarliges eget bruk.

Disse medlemmer er av den oppfatning at også selve formålet med registreringen kan påvirke nødvendighetsnormen. Pol. § 11 b har lovfestet det såkalte finalitetsprinsippet, som innebærer at det er et krav om at formålet må være uttrykkelig angitt og saklig begrunnet. Hensikten er at hvis den behandlingsansvarlige har fulgt bestemmelsen, vil det være lettere å vurdere kravet til nødvendighet. Finalitetsprinsippet er ikke utelukkende et krav om å fastsette formålet i en konkret behandlingssituasjon, men inneholder også et saklighetskrav, og et krav til at behandlingen ikke senere skal komme i motstrid til formålet. Prinsippet inneholder ytterligere krav om konkretisering som har nær sammenheng med angivelsen av formålet. Formålet med registreringen skal angis så veldefinert og avgrenset at det skaper klarhet og åpenhet om behandlingen.

Disse medlemmer mener ovennevnte drøftelse burde vært gjort grundigere i relasjon til gjenbruksproblematikken, og vil derfor reservere seg mot meldingens omtale av gjenbruk av data, da denne omtalen mangler en tilfredsstillende problematisering.

Komiteens medlemmer fra Fremskrittspartiet mener at et sterkt personvern også

må gjelde på den enkelte arbeidsplass. Prinsippet «need to know» må kun praktiseres i de tilfeller der det er helt nødvendig eller ved mistanke om noe straffbart eller brudd på regler. Disse medlemmer mener arbeidstakere skal føle seg trygge på at de ikke blir ulovlig overvåket eller at uvedkommende får innsyn i deres personalia eller andre opplysninger som omhandler dem, uten at det er gitt samtykke til dette.

4. Gjenbruk av personopplysningar

4.1 Sammendrag

4.1.1 Generelt om personvernutfordringar ved gjenbruk av personopplysningar

4.1.1.1 Innleiing

Ønske om gjenbruk av data er eit meir og meir aktuelt tema.

Det blir i meldinga vist til at slik gjenbruk ofte er eit gode, men kan òg føre til at personvernet blir utfordra. Det blir derfor stadig viktigare å vurdere om, og eventuelt i kva omfang, gjenbruk av personopplysningar er akseptabelt.

4.1.1.2 Kva er gjenbruk?

Med gjenbruk av personopplysningar forstår ein i denne meldinga bruk av personopplysningar til eit anna føremål enn det opphavlege innsamlingsføremålet eller til bruk hos ein annan behandlingsansvarleg enn den som er ansvarleg for primærbehandlinga.

Som for primærbehandlinga må ein ha eit rettsleg grunnlag (behandlingsgrunnlag) for gjenbruken.

Dersom føremålet med innsamling og behandling av personopplysningar er at opplysningane skal gi grunnlag for bruk til fleire føremål eller av fleire verksemder, blir det ikkje kalla gjenbruk i meldinga. Andre gonger er ny bruk ikkje noko ein tenkte på då ein samla inn personopplysningane første gongen. Om ny behandling av opplysningane følgjer av den opphavlege innsamlingsheimelen, slik at den også kan danne rettsleg grunnlag for ny bruk, vil då kvile på ei tolking av rettsgrunnlaget.

Somme gonger kan lovheimla teieplikt vere ein skranke for gjenbruk av personopplysningar.

Der ein finn at gjenbruk av innsamla personopplysningar er ønskjeleg, anten av omsyn til dei registrerte eller av omsyn til samfunnet, kan lovgivaren fastsetje reglar som opnar for den gjenbruken ein ønskjer. Behandling av opplysningar som skjer i tråd med det nye behandlingsgrunnlaget, vil då ikkje lenger vere gjenbruk av personopplysningar slik omgrepet blir nytta i denne meldinga. Lovreglar om gjenbruk vil òg kunne setje til side ei eventuell teieplikt. Slik legg ein til rette for gjenbruk av viktige personopplysningar til beste for den registrerte sjølv, for samfunnet eller for begge partar.

4.1.1.3 Generelt om gjenbruk og personvern

Gjenbruk av personopplysningar kan ofte ha store fordelar, både for den einskilde og for samfunnet. Gjenbruk er ofte i tråd med interessene til den registrerte.

Regjeringa ønskjer at digital kommunikasjon skal vere hovudregelen for kommunikasjon med forvaltninga, og dette er eit av prinsippa i digitaliseringsprogrammet til regjeringa.

Gjenbruk kan vidare vere viktig for å sikre samfunnsinteresser og interesse for private aktørar.

Sjølv om gjenbruk av personopplysningar i mange samanhengar er både nyttig og nødvendig, reiser det likevel særlege spørsmål om ivaretaking av personvernet. Ei gjenbruksvurdering inneheld ofte litt andre moment og omsyn enn ei vurdering av primærbruk av personopplysningar. Derfor er det viktig å gjere ei ny vurdering av personvernkonsekvensar ved gjenbruk av personopplysningar. Plikta til å vurdere personvernkonsekvensar er den same uansett om det gjeld primærbruk eller gjenbruk. Det er likevel viktig å minne særskilt om plikta i samband med gjenbruk, fordi ho kan verke mindre klår i ein situasjon der opplysningane allereie er innsamla. Ved gjenbruk kan òg nye moment kome fram ved vurderinga.

Det går fram av personopplysningslova § 11 første leddet bokstav c) at personopplysningar:

> «ikke [kan] brukes senere til formål som er uforenelige med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker».

Men òg i situasjonar der den nye bruken kan synast å stå i strid med det opphavlege innsamlingsføremålet, kan ein leggje til rette for gjenbruk gjennom å vedta lovheimlar for den nye bruken.

4.1.1.4 Særleg om lovfesta rett til gjenbruk

Det blir i meldinga vist til at gjenbruk av personopplysningar ofte er ønskjeleg ut frå eit samfunnsperspektiv. Gjenbruk krev likevel eit nytt behandlingsgrunnlag. For det offentlege vil lov ofte vere det best eigna behandlingsgrunnlaget. Innhenting av samtykke til ny behandling frå alle dei registrerte kan vere krevjande og i mange tilfelle òg lite tenleg. Ein kan òg tenkje seg tilfelle der den registrerte ikkje ønskjer å gi samtykke, men der tilgang til opplysninga likevel er ønskjeleg og nødvendig for å ta vare på andre interesser. I slike tilfelle blir gjenbruk fastsett i lov.

Personopplysningslova gjeld for behandling av personopplysningar «om ikke annet følger av en sær-

skilt lov som regulerer behandlingsmåten», jf. personopplysningslova § 5. Dette må ein likevel, som ved anna lovfesting, sjå i samanheng med EMK artikkel 8, som seier at staten ikkje kan gjere inngrep i utøvinga av retten til privatliv med mindre det er i samsvar med lova og er «nødvendig» i eit demokratisk samfunn av gitte omsyn.

I Soria Moria II skriv regjeringa at:

«[p]ersonvernet kan komme i konflikt med andre formål. Regjeringen vil ha fokus på at personvernet ikke svekkes. Det må etableres ordninger som både tar hensyn til samfunnets behov for innsyn og kontroll og enkeltmenneskets rett til personvern.»

Ved lovfesting av gjenbruk av personopplysningar er det derfor viktig at lovgivaren gjer ei grundig utgreiing av personvernkonsekvensar i lovgivingsprosessen. Dette er klårgjort ved at personvern er teke inn som eit eige punkt 11.3.11 i rettleiinga til utgreiingsinstruksen, samt ei eiga rettleiing av personvernkonsekvensar.

4.1.2 Kriminalitetsførebygging

4.1.2.1 Utfordringar ved gjenbruk av informasjon innhenta av politiet

Politiet hentar inn mange personopplysningar som eit ledd i innsatsen mot kriminalitet. I somme tilfelle er den registrerte uvitande om at det blir innhenta opplysningar om han eller henne. Det hender òg at den som gir opplysningar til politiet, har direkte interesse i at opplysningane politiet får, ikkje er korrekte.

Desse særeigne tilhøva når politiet hentar inn informasjon, fører med seg at opplysningane ofte er meir usikre enn hos andre forvaltningsorgan. Kvalitetssikring av opplysningar har noko å seie for spørsmålet om korleis opplysningane skal nyttast vidare, medrekna om dei skal utleverast til andre offentlege organ eller ålmenta.

I politiregisterlova er det gitt nærmare reglar om korleis utlevering av ikkje-verifiserte opplysningar bør skje. Det går mellom anna fram at det skal opplysast at opplysningane er usikre.

4.1.2.2 Gjenbruk av informasjon innhenta som forvaltningsorgan

Det kan kome spørsmål om opplysningar som politiet har innhenta som forvaltningsorgan, kan nyttast i innsatsen mot kriminalitet.

Forvaltningsregistra til politiet fell ikkje inn under reglane i politiregisterlova, men er regulerte av personopplysningslova. Eit grunnleggjande prinsipp i den generelle personvernlovgivinga er at opplysningar som er innhenta til eit visst føremål, ikkje skal nyttast til andre føremål. I utgangspunktet har politiet derfor ikkje rett til å nytte opplysningar innhenta til forvaltningsføremål ved gransking av lovbrot. Straffeprosesslova gir likevel politiet heimlar til å hente ut informasjon frå ulike forvaltningsregister på nærmare fastsette vilkår. Kor alvorleg lovbrotet er, har noko å seie for om det er høve til å hente ut informasjon.

4.1.2.3 Gjenbruk av informasjon innhenta ved politiarbeid

Etter reglane i straffeprosesslova er opplysningar innhenta ved gransking underlagde teieplikt. Opplysningane kan likevel nyttast fritt i samband med gransking og gjennomføring av ei straffesak. Informasjon som er innhenta ved bruk av granskingsmetodar heimla i straffeprosesslova kapittel 16 a, for eksempel kommunikasjonskontroll, er likevel underlagd ei særleg teieplikt etter straffeprosesslova § 216 i. Det er òg ei særskild teieplikt om overskotsinformasjon innhenta av Politiets tryggingsteneste (PST) med tanke på førebygging etter politilova § 17 d.

I NOU 2009:15 Skjulte metoder – åpen kontroll gjer fleirtalet i Metodekontrollutvalet framlegg om å endre reglane som gjeld i dag, slik at det blir mogleg å nytte såkalla «overskotsinformasjon» etter bruk av tvangsmiddel som bevis i rettssaker, også der det er tale om mindre alvorlege lovbrot.

Justis- og beredskapsdepartementet arbeider for tida med oppfølginga av rapporten frå Metodekontrollutvalet, medrekna utarbeiding av ein lovproposisjon.

4.1.3 Bruken av personopplysningar for kontrollføremål i Arbeids- og velferdsetaten

Det blir i meldinga vist til at Arbeids- og velferdsetaten må ta vare på den vanskelege balansegangen mellom personvern og kontroll med om vilkåra for folketrygdytingar er oppfylte eller har vore oppfylte, i tidlegare periodar. Arbeids- og velferdsetaten forvaltar vide fullmakter til å hente inn opplysningar frå nærmare avgrensa grupper. Reglane som gjeld i dag, er av relativt ny dato, og dei har vore ute på ein vidfemnande høyringsrunde. Avvegingane mellom personvernomsyn og kontrollbehov var hovudtema i mange av høyringsinnspela. Personvernomsyn vart derfor ein sentral del av vurderingane departementet gjorde. I meldinga blir det sitert frå proposisjonen, Ot.prp. nr. 76 (2007–2008).

I innstillinga til Odelstinget, Innst. O. nr. 35 (2008–2009), viser samstundes arbeids- og sosialkomiteen til kva velfungerande kontroll har å seie for å ta vare på tilliten til trygdesystemet.

Arbeidsdepartementet har nyleg varsla Stortinget om at reglane for kontrollverksemda til Arbeids- og velferdsetaten skal vurderast, mellom anna i lys av påpeikingar i ein kontrollrapport frå Datatilsynet.

4.1.4 Marknadsføring

Krav om innhenting av førehandssamtykke ved elektronisk marknadsføring følgjer av EU-direktivet om kommunikasjonsvern (2002/58/EF) og er ein modell som er kjend frå store delar av verda. Når det gjeld marknadsføring ved hjelp av telefon eller direkteadressert post, er det berre stilt minimumskrav gjennom EU-lovgivinga. Det har derfor vore drøfta på nasjonalt plan om ei løysing med eit reservasjonsregister gir personar tilstrekkeleg vern mot uønskte marknadsføringsførespurnader, eller om det for eksempel bør innførast eit krav om samtykke for å kunne rette særleg telefonførespurnader til forbrukarar med tanke på marknadsføring.

Omsyna som har stått mot einannan i dette ordskiftet, har først og fremst vore omsynet til å verne privatlivet på den eine sida og omsynet til å gi næringsdrivande og humanitære organisasjonar enkel tilgang til ein salskanal på den andre. Ønsket om å verne om arbeidsplassar i distrikta har òg vore vektlagt. Det vart i samband med vedtaket om ny marknadsføringslov i 2009 avgjort at ordninga med eit reservasjonsregister for personar som ikkje ønskjer telefonsal og direkteadressert marknadsføring, skulle vidareførast, og at ordninga skulle evaluerast over ein periode på fem år. Talet på skriftlege klager til Forbrukarombodet frå personar som opplever å bli oppringde trass i at dei har reservert seg mot telefonsal, er framleis høgt.

Med den elektroniske informasjonsutviklinga dei siste tiåra, har det å kunne rette marknadsføring direkte til forbrukarar gjennom elektroniske kanalar, for eksempel e-post og sosiale medium, vorte stadig viktigare for næringslivet. Krav som pålegg næringsdrivande å hente inn samtykke før dei vender seg direkte til personar gjennom dei elektroniske kommunikasjonskanalane dei nyttar, er heilt nødvendig.

Det blir i meldinga peikt på at det med det jamt aukande talet på næringsdrivande forbrukarane kommuniserer elektronisk med, blir stadig viktigare med klåre grenser for korleis aktørane kan nytte personopplysningane dei tek imot, og at desse grensene blir vakta. Frå tilsynsarbeidet hos Datatilsynet og Forbrukarombodet er det ei lang rekkje eksempel på at næringsdrivande lagrar personopplysningar dei ikkje skulle ha lagra, og nyttar desse på ein måte som lova ikkje tillèt.

Lovstridig gjenbruk av personopplysningar til elektronisk marknadsføring er noko som kan føre med seg inngrep i privatsfæren til mange personar. Særleg uheldige blir inngrepa dersom næringsdrivande sender ut meldingar på SMS som forbrukarane betaler for å ta imot, såkalla overtaksert SMS.

Lovstridig gjenbruk av personopplysningar til marknadsføring kan sannsynlegvis kome av både mangel på kunnskap om regelverket og manglande vilje til å innrette seg etter det. Både Datatilsynet og Forbrukarombodet bruker ressursar på å spreie informasjon om regelverket og føre tilsyn med at det blir følgt.

Når personopplysningar blir nytta til å rette marknadsføring til forbrukarar ved hjelp av telefon og direkteadressert post er innhenting av grunndata (opplysningar om namn, adresse, fasttelefonnummer og fødselsdato) unnatekne frå kravet i personopplysningslova om samtykke ved innhenting av personopplysningar.

4.1.5 Helse- og omsorgssektoren

Å behandle helseopplysningar er nødvendig for å kunne yte god helsehjelp til den registrerte. For å kunne yte så gode helse- og omsorgstenester som mogleg til innbyggjarane som heilskap og for å kunne yte betre tenester av høgare kvalitet til kvar einskild innbyggjar, er det òg ønskjeleg og ofte nødvendig, å bruke journalopplysningar til føremål som kvalitetstrygging, forsking, styring og helseovervaking. Slik gjenbruk føreset ei grundig vurdering av kva konsekvensar bruken kan få for ivaretakinga av interessene til den einskilde. På helseområdet blir gjenbruk av helseopplysningar til andre føremål enn å yte helsehjelp omtala som «sekundærbruk av helseopplysningar», medan bruk mellom verksemder ikkje blir omfatta av omgrepet. Det er viktig at relevante helseopplysningar kan følgje pasientar og brukarar i ei behandlingsrekkje, og det er såleis lite eigna å kalle denne informasjonsflyten for gjenbruk. Informasjonsflyt på helseområdet er derfor særskilt regulert for å sikre slik bruk.

Det blir i meldinga vist til at gjenbruk av helseopplysningar er avgjerande for å kunne halde oversikt over førekomsten av ulike sjukdomar og for forsking på sjukdomsårsaker og behandlingseffektar.

Gjenbruk av helseopplysningar ved etablering av helseregister kan etter omstende opplevast som eit inngrep i personvernet til den einskilde. Helseregister er likevel i mange tilfelle positive for personvernet til pasienten og brukaren.

Det blir i meldinga peikt på at nytta av helseregister bør vere stor, og ho bør vege opp ein eventuell personvernrisiko. I motsetnad til det som er tilfellet ved yting av helsehjelp, er det ei utfordring å gjere denne avveginga synleg ved oppretting av helseregister. Registeret gagnar likevel dei registrerte (pasientane) i form av meir kunnskap og betre helsehjelp. Ikkje minst gjeld dette pasientgrupper med kroniske sjukdomar.

Det er ei tilbakevendande utfordring at samtykkebasert registrering i helseregister kan gi for dårleg og/eller skeiv representativitet. Stortinget har lagt til grunn at enkelte sentrale helseregister ikkje bør tuftast på samtykke fordi eit samtykkekrav fører til pro-

blem med representativitet, ufullstendig innhald og for dårleg datakvalitet (sjå m.a. Ot.prp. nr. 49 (2005–2006)). God representativitet og datakvalitet er ein føresetnad for at registera skal kunne tene føremålet.

Regjeringa meiner at gjenbruk av helseopplysningar i helseregister er nødvendige og gode verkemiddel for å få oppdatert og påliteleg kunnskap om helsetilstand, helsetenester og årsaker til sjukdom. Ved oppretting av register må det likevel alltid gjerast ei avveging mellom behovet og nytta samfunnet har av gjenbruk, og behova den registrerte har for personvern.

4.1.6 Forsking

4.1.6.1 Forsking og kunnskapsbehovet i forvaltninga

I kraft av si rolle som tenestetilbydar lagrar forvaltninga store mengder personopplysningar. Arkivlova stiller krav om at materialet skal oppbevarast, og opplysningsmassen utgjer eit svært godt utgangspunkt for å få ny kunnskap.

Utan god informasjon om tenesteområda, kan staten vanskeleg oppfylle sitt tilretteleggings- og styringsansvar. For at behovet for informasjon skal bli oppfylt, står valet i all hovudsak mellom tre datakjelder: utvalsundersøkingar, statistikk innsamla på ulike aggregerte nivå og statistikk basert på personeintydige opplysningar.

Det offentlege har eit stort behov for å gjennomføre evalueringar av effekten av statlege og lokale verkemiddel. I dei fleste tilfelle krev slike evalueringar personeintydige opplysningar og helst med fleire måletidspunkt (longitudinelle studiar). Utan personopplysningar vil kunnskapsgrunnlaget for statleg styring bli langt svakare, og det vil vere vanskelegare å byggje opp eit kunnskapsgrunnlag om dei ulike sektorane og om kva som verkar, og kva som ikkje verkar effektivt. Det er òg naturleg å vise til at innbyggjarane har ei viss forventing om at staten faktisk gjenbruker informasjon i denne samanhengen.

I mange tilfelle vil passiv deltaking i forsking gjennom studiar av allereie eksisterande register representere eit uvesentleg trugsmål mot fridomen og privatlivet til individa. Men slik gjenbruk av personopplysningar krev vanlegvis samtykke dersom registerstudiane skal supplerast med informasjon henta gjennom aktiv kontakt med informantane, eller dersom forskinga genererer nye, sensitive opplysningar om einskildpersonar som kan identifiserast. Reine registerstudiar kan ofte baserast på andre rettslege grunnlag, men dei registrerte vil framleis ha krav på informasjon om prosjektet.

Identifiserbare personopplysningar, innsamla for eitt bestemt forskingsføremål, kan ikkje utan vidare nyttast til anna forsking, og dei skal ikkje brukast til kommersielle føremål eller forvaltningsføremål. Dette kravet byggjer på respekten for fridomen og privatlivet til individet. Ved gjenbruk av personidentifiserbare opplysningar går ein vanlegvis ut frå at dei undersøkte har gitt samtykke. Dette gjeld likevel ikkje for anonymiserte data.

4.1.6.2 Fordelar og utfordringar ved gjenbruk

Gjenbruk av personopplysningar må ha eit eige behandlingsgrunnlag.

For forskingsprosjekt vil det ofte vere nødvendig med dispensasjon frå teieplikta for å få tilgang til informasjonen.

Statistikk basert på personeintydige opplysningar er i mange tilfelle meir kostnadseffektiv enn statistikk basert på ulike aggregerte nivå og utvalsundersøkingar. Statistikk basert på personeintydige opplysningar held dessutan generelt sett høgare datakvalitet enn statistikk som er innsamla på ulike aggregerte nivå.

Gjenbruk av allereie innsamla personopplysningar er derfor nyttig for forskinga. Opplysningane er knytte direkte til tenesteytinga i kvar einskild sektor og er derfor særleg relevante.

I personopplysningslova er hovudregelen at gjenbruk som ikkje svarar til det opphavlege innsamlingsføremålet, ikkje er tillate. Ein omfattande, lovheimla rett til gjenbruk kan setje dette prinsippet under sterkt press.

Både statistikk og forsking er i personopplysningslova vurderte som legitime behandlingsføremål, jf. personopplysningslova § 11.

Kvar gang gjenbruk skjer må det gjennomførast ei proporsjonalitetsvurdering. Personvernnemnda har i fleire av avgjerdene sine framheva at samfunnet har interesse av at forsking og analysar blir gjennomførte, medrekna at desse blir baserte på allereie eksisterande data.

Vurderinga viser at lovgivaren har sett på bruk av personopplysningar til statistikk og forsking med andre auge. Regjeringa meiner at dette, samanhalde med prinsippet om gjenbruk av offentleg finansierte forskingsdata, tilseier ei vidareføring av den noko meir liberale praksisen det offentlege har følgt når det gjeld gjenbruk av data for forsking, styring og administrasjon av dei sektorane som det offentlege har ansvar for.

4.1.7 Gjenbruk av opplysningar i arbeidslivet

Det blir i meldinga vist til at gjenbruk av opplysningar i arbeidslivet er ei stadig aukande utfordring, og i rettstvistar om oppseiing/avskilssaker kjem av og til spørsmålet om gjenbruk av opplysningar opp. Hovudregelen er at personopplysningane berre kan nyttast til føremål som er uttrykkeleg og sakleg grunngitte i verksemda til den behandlingsansvar-

lege. Hovudregelen i tvistemålslova er fri bevisføring. Retten kan likevel i særlege tilfelle nekte føring av bevis som er skaffa på utilbørleg måte.

Tendensen synest å vere at avdekking av kriminalitet og avkrefting av mistanke mot uskyldige er legitime føremål for eit kontrolltiltak. Grunngitt mistanke veg òg tungt ved vurdering av om eit tiltak er rimeleg.

Skjult overvaking, for eksempel hemmeleg kameraovervaking, blir normalt rekna som ulovleg.

Tradisjonelle kontrolltiltak, som veskekontroll og kontrollkjøp, synest å liggje innanfor arbeidsgivaren sin kontrolltilgang. Bruk av GPS-loggar, som er diskutert og avtala med arbeidstakaren, for eksempel for å leggje opp køyreruter, synest òg i rettspraksis å vere rekna som eit slikt tradisjonelt kontrolltiltak som ikkje krenkjer personvernet. Ein går likevel ut frå at tiltaket må vere knytt til føremålet og innført på ein korrekt måte, blant anna gjennom informasjon og drøfting med dei tilsette. I slike tilfelle har det vore gitt høve til gjenbruk av opplysningane som bevis i rettssaker om oppseiing og avskil.

Fleire avgjerder i rettstvistar tyder på at etterleving av saksbehandlingsreglane ved innføring av kontrolltiltak kan vere avgjerande for om retten ser på framlagde bevis som innhenta på rett vis, og dermed om dei kan førast som bevis i ei sak for domstolane.

Det finst likevel òg avgjerder der domstolen har tillate arbeidsgivaren å føre bevis som er skaffa på ulovleg vis.

4.1.8 Dokumentasjonsplikt og dokumentasjonsbehov for ettertida

4.1.8.1 Tilhøvet til ulike oppbevaringsplikter

Arkivlova og pliktavleveringslova inneheld reglar om bevaring og tilgjengeleggjering av allereie produsert, og til dels tilgjengeleggjort, materiale.

I den grad personopplysningar er omfatta av lovene, dreiar det seg om bevaring, og eventuelt tilgjengeleggjering, av dei personopplysningane som er ein del av dei bevarte dokumenta.

Ein grunnleggjande føresetnad for ytringsfridom er retten til relevant informasjon, og offentleg transparens går ut på at dokumenta som dannar grunnlag for offentlege avgjerdsprosessar, skal takast vare på for ettertida.

4.1.8.2 Arkivregelverk

Arkivlova gjeld i all hovudsak for offentlege institusjonar.

Som hovudregel kan ikkje (offentleg) arkivmateriale kasserast (destruerast) utan samtykke frå Riksarkivaren. Arkivlova § 9 inneheld likevel ei særskild presisering om at pålegg om sletting av personopplysningar gitt med heimel i personopplysningslova § 28 eller helseregisterlova §§ 7, 8, 26 og 28 uansett gjeld uavgrensa etter at Riksarkivaren har fått uttale seg.

For store delar av arkivbestanden i offentleg forvaltning gjeld publikums rett til innsyn.

Alle arkiv er pålagde å rette seg etter teiepliktreglane som er fastsette i ei rekkje ulike lover.

I personopplysningslova bruker ein ikkje omgrepet teieplikt, men lova gir påbod om å setje i verk tiltak for å sikre tilstrekkeleg fortruleg behandling. Forvaltningsorgan og arkivdepot må rette seg etter dei krav som følgjer av personopplysningslova med forskrifter. Dette set grenser for kva som kan gjerast fritt tilgjengeleg, og dessutan for korleis materiale kan formidlast.

Då teiepliktreglar vart tekne inn i forvaltningslova frå 1. januar 1978, var det ein føresetnad at desse reglane ikkje skulle gjere det vanskelegare enn før å drive samfunnsnyttig forsking. Det vart derfor teke inn ein regel i forvaltningslova om at teieplikta ikkje skulle vere til hinder for at forskarar kan få tilgang til opplysningar som er underlagde teieplikt. Føresetnaden var at forskaren òg skulle ha teieplikt.

4.1.8.3 Pliktavleveringslova

Det er ein føresetnad for pliktavlevering at materialet både er allment tilgjengeleg, og at det er relevant for Noreg. Vidare skal tilgjengeleggjering av materialet gjerast for forsking og dokumentasjon, som inneber at pliktavlevert materiale som utgangspunkt ikkje er allment tilgjengeleg.

4.1.9 Hovudpunkt kapittel

- Tilrettelegging for gjenbruk av data står sentralt i politikken til regjeringa. Der data inneheld personopplysningar, må ein likevel vere varsam ved gjenbruk.
- Det bør leggjast vekt på varsling til dei registrerte ved gjenbruk av opplysningar til kontrollføremål.
- Ved oppretting av forskings- og helseregister må samfunnet sitt behov for og nytte av gjenbruk vegast mot den registrerte sitt behov for personvern. Personvernkostnadene bør vere så låge som mogleg, og reservasjonsordningar bør vurderast.
- Det bør vurderast klårare regulering av arbeidsgivaren sin rett til å gjenbruke opplysningar om ein arbeidstakar til andre føremål enn det opphavlege innsamlingsføremålet.

4.2 Komiteens merknader

Komiteen vil peke på at det i grunnprinsippet for lagring av opplysninger som kan knyttes til enkeltpersoner ligger en begrensning i formålet med

registreringen. Gjenbruk av opplysninger er derfor i utgangspunktet det samme som bruk av opplysninger utover de normale grenser personvernet setter. Det må derfor avklares nærmere på hvilket grunnlag en skal kunne tillate dette. Plikten til å vurdere personvernkonsekvenser for den enkelte gjelder like mye enten det gjelder primærbruk eller gjenbruk av opplysninger.

Komiteen viser til drøftelsen om at gjenbruk av opplysninger kan være særlig aktuelt ved forebygging av kriminalitet og kontroll med at betingelsene for sosiale ytelser er til stede, foruten forskning og markedsføring. Komiteen vil understreke at det er en betydelig oppgave å informere om hvordan opplysninger evt. kan bli gjenbrukt, og en vil være tilbøyelig til å akseptere mer gjenbruk hvis det i utgangspunktet er informert om muligheten for kontroll, og motparten har en reell mulighet til å velge.

Komiteens medlemmer fra Fremskrittspartiet, Høyre og Kristelig Folkeparti finner omtalen av prinsippene for gjenbruk lite klargjørende, først og fremst fordi man bringer seg i motsetningsforhold til personopplysningsloven § 11 bokstav c, som forutsetter samtykke når personopplysninger brukes i annen sammenheng enn de var innhentet for.

Disse medlemmer oppfatter drøftelsen om forholdet til EMK Art 8 som begrenset til et spørsmål om å skaffe seg lovhjemmel, gjerne i ettertid, for slik utvidet bruk. Artikkel 8 krever lovhjemmel, men knytter til vilkåret om at eventuell lovhjemmel må være båret av sterke samfunnsmessige hensyn – «pressing social need». Dette innebærer at gjenbruk må begrunnes ut fra sterke samfunnsmessige behov, ikke bare at det er praktisk eller arbeidsbesparende.

5. Vilkår for behandling av personopplysningar

5.1 Sammendrag

5.1.1 Generelt om det rettslege grunnlaget for behandling av personopplysningar

Det går fram av meldinga at behandling av personopplysningar kan ha grunnlag i samtykke frå dei registrerte, i lovheimel eller i ein av dei nærmare bestemte grunnane i personopplysningslova § 8 bokstavane a til f. Når ein skal behandle sensitive personopplysningar, må ein ha grunnlag i både § 8 og § 9. Dette inneber at det blir stilt strengare krav til heimelsgrunnlag ved behandling av personopplysningar som er sensitive, enn ved behandling av andre personopplysningar.

Behandling av personopplysningar er nødvendig for eit velfungerande samfunn og ein føresetnad for rettsstaten. Ein må kunne samle inn personopplysningar til definerte føremål og kunne bruke opplysningane til desse føremåla. Når det gjeld krav til rettsleg grunnlag for behandling av personopplysningar, er det stor forskjell mellom offentlege styremakter, private aktørar som utfører lovheimla offentlege tenester og oppgåver, og private aktørar. Privatrettsleg bind innbyggjarane seg frivillig ved avtalar, medan myndigheita på det offentlegrettslege området er knytt til lovgiving. Utøving av offentleg myndigheit er bindande utan noka form for samtykke frå innbyggjarane.

Det blir i meldinga vist til at det er ønskjeleg at dei registrerte har så stor råderett over eigne personopplysningar som mogleg. Samtykke som behandlingsgrunnlag står sentralt i denne samanhengen. I den vidare framstillinga vil spørsmålet om lovheimel som behandlingsgrunnlag i første rekkje vere knytt til utføring av lovpålagde offentlege oppgåver, sjølv om dette òg er eit aktuelt behandlingsgrunnlag for private aktørar i visse samanhengar. Samtykke som behandlingsgrunnlag er primært aktuelt i privat sektor, men kan òg vere relevant i offentleg sektor. Enkelte personopplysningsbehandlingar er openbert nødvendige for å utføre lovpålagde offentlege oppgåver, sjølv om behandlinga ikkje har nokon eksplisitt heimel i lov. Då må ein kunne leggje til grunn at lovgivaren har vurdert dei personvernmessige konsekvensane av lova, og at den medfølgjande behandlinga ikkje er så inngripande at ho etter legalitetsprinsippet krev ein klårare lovheimel. Nødvendiggjerande grunnar kan vere aktuelle behandlingsgrunnlag i både offentleg og privat sektor. I offentleg sektor vil til dømes utøving av offentleg myndigheit eller utøving av oppgåver av allmenn interesse kunne vere aktuelle grunnlag for innsamling og bruk av personopplysningar. I privat verksemd kan ein aktuell grunn vere oppfylling av ei avtale med den registrerte.

5.1.2 Val av behandlingsgrunnlag

Dei tre behandlingsgrunnlaga samtykke, lovheimel og grunn som gjer behandling nødvendig er likeverdige alternativ i personopplysningslova.

I valet mellom samtykke eller nødvendiggjerande grunn som grunnlag for behandling av personopplysningar, går det fram av forarbeida til personopplysningslova at personopplysningsbehandlingar i størst mogleg grad bør baserast på samtykke der dette let seg gjere.

I ei rekkje samanhengar er samtykke likevel ikkje eit eigna grunnlag for behandling av personopplysningar. Behandling av personopplysningar i offentleg forvaltning er i stor grad basert på heimel i lov som ein føresetnad for utøving av offentleg myndigheit eller som ein føresetnad for å utøve ei lovpålagd offentleg oppgåve.

For private aktørar kan det òg vere nødvendig å nytte andre behandlingsgrunnlag enn samtykke. Eit eksempel kan vere behandling av kontaktinformasjon for bruk i direkte marknadsføring. Behandling av kontaktinformasjon er i dei fleste tilfelle lite personverninngripande, og det å bli kontakta for direkte marknadsføring er ikkje eit stort personverninngrep for den enkelte. På den andre sida kan kostnaden ved å innhente samtykke for slike behandlingar vere stor i høve til gevinsten.

5.1.3 Lovheimel og nødvendiggjerande grunn som grunnlag for behandling av personopplysningar

Forvaltninga si innsamling og bruk av personopplysningar er i hovudsak fastsett i lov eller er nødvendig for å utøve offentleg myndigheit. Tilsvarande gjeld for private aktørar som utfører lovpålagde offentlege tenester. Forvaltninga si behandling av personopplysningar må sjåast i samanheng med at behandling av personopplysningar ofte skjer som del av utøvinga av myndigheit. Personopplysningane som blir behandla, må vere relevante og oppdaterte. Langt på veg har derfor det offentlege og dei registrerte dei same interessene når grunnlag for behandling av personopplysningar skal vurderast.

Det blir i meldinga vist til at samtykke er eit lite eigna behandlingsgrunnlag for dei fleste behandlingar av personopplysningar i forvaltninga.

Somme lover regulerer sjølve behandlinga av personopplysningar, og behandlinga kan stå fram som eit mål i seg sjølv.

Sidan forvaltninga si utøving av myndigheit byggjer på legalitetsprinsippet, følgjer det av heimel i lov kva oppgåver offentlege styremakter skal utføre. Ein må leggje til grunn at lovgivaren òg har vurdert personvernsidene ved ei vedteken forvaltningsordning som krev at visse personopplysningar blir behandla.

Lovheimel som behandlingsgrunnlag kan ein ha både der det direkte er gitt heimel til å behandle personopplysningar, og der det er føresett at slik behandling kan skje. Tilsvarande gjeld for private aktørar som utfører lovpålagde offentlege tenester. Kva opplysningar som er dekte av heimelen, må likevel avgrensast til det som er nødvendig og relevant, slik at kravet til forholdsmessigheit og dataminimalitet i personopplysningslova blir oppfylt.

Det går fram av meldinga at dersom ei grundig vurdering etter legalitetsprinsippet viser at ei personopplysningsbehandling i offentleg verksemd ikkje har slik heimel i lov at lovkravet i personopplysningslova er oppfylt, må ein sjå om personopplysningslova gir eit anna behandlingsgrunnlag. I slike tilfelle må forvaltninga kunne behandle personopplysningar med heimel i personopplysningslova § 8 bokstav e, når det er nødvendig for «å utøve offentlig myndighet».

I behandlinga av utkastet til ny personvernforordning i EU er det peikt på at den nødvendiggjerande grunnen i personopplysningslova § 8 bokstav e er det mest sentrale behandlingsgrunnlaget for offentlege styremakter. Dersom forvaltningsorganet ønskjer å samle inn opplysningar som ikkje er relevante for utøving av myndigheit, for eksempel ei brukarundersøking, kan behandlinga ikkje heimlast i § 8 bokstav e.

I meldinga blir det peikt på at i framtida bør behandling av personopplysningar som er ein nødvendig føresetnad for at den offentlege forvaltninga kan utøve myndigheit og utføre tenester, så langt råd er ha heimel i lov. Utgreiingar av personvernkonsekvensar i lovgivingsprosessen kan bidra til auka merksemd på behovet for og innretninga av personopplysningsbehandlinga og såleis gi eit betre regelverk og eit betre personvern.

5.1.4 Samtykke som behandlingsgrunnlag

Samtykke blir i mange samanhengar framheva som det føretrekte grunnlaget for behandling av personopplysningar.

5.1.4.1 Ulike typar samtykke

Krava til eit samtykke i personvernsamanheng er lovregulert. Etter personopplysningslova § 2 nr. 7 skal eit samtykke vere ei frivillig, informert og uttrykkeleg erklæring frå den registrerte om at vedkomande godtek behandling av opplysningar om seg sjølv. Samtykket skal vere ei aktiv handling frå dei registrerte si side. Det er ikkje eit krav at samtykket blir gitt skriftleg. Det er likevel den behandlingsansvarlege som har ansvaret for å dokumentere at det er gitt eit gyldig samtykke.

Før han eller ho gir samtykke, skal den registrerte få god og forståeleg informasjon om bruken av personopplysningar. Informasjonen skal seie noko om føremålet med behandlinga, kva opplysningar som blir behandla, og korleis dei blir henta inn, i tillegg til kven som har tilgang til opplysningane. Denne informasjonen skal danne grunnlaget for samtykket og vil vere avgjerande for kor langt samtykket rekk.

Informasjonen må vere godt synleg og lett tilgjengeleg for brukaren, helst samla på éin stad. Ein bør unngå å bruke vanskeleg språk og lange formuleringar. For mykje informasjon kan føre til at brukaren føler avmakt og unngår å setje seg inn i informasjonen, medan for lite informasjon kan føre til at brukaren ikkje forstår omfanget av behandlinga han eller ho samtykkjer i. Begge situasjonane kan føre til at samtykket ikkje tilfredsstiller krava i lova. Dei europeiske datatilsynsstyremaktene synest å vere einige om at ein gjennomsnittleg brukar bør vere i stand til

å forstå informasjonen for at den skal vere tilfredsstillande.

Samtykket skal vere frivillig. Det blir i meldinga vist til at dersom det kan vere tvil om den registrerte opplever å ha eit reelt val, bør ikkje behandling av personopplysningar ha grunnlag i samtykke.

Det blir i meldinga vist til at alternativ til samtykke kan vere reservasjonsrett eller implisitt samtykke/konkludent åtferd.

Implisitt samtykke og konkludent åtferd

Det er viktig å skilje mellom samtykke til å delta i ei gitt handling eller aktivitet og samtykke til behandling av personopplysningar som følgjer av denne aktiviteten.

«Clickwrap» er ein avtale som blir inngått på nett ved at standardvilkår blir presenterte for brukaren i eit eige vindauge, og brukaren aksepterer desse vilkåra ved for eksempel å klikke på ein «aksept»-knapp.

Både Datatilsynet og Forbrukarombodet legg til grunn at «click-wrap»-samtykke ikkje oppfyller krava til samtykke etter personopplysningslova og marknadsføringslova mellom anna fordi informasjonen er mangelfull. Forbrukarombodet har det siste året prioritert å få rydda opp i bruk av «clickwrap»-samtykke som grunnlag for behandling av personopplysningar i marknadsføringssektoren. Tilsyn og informasjon til behandlingsansvarlege kan bidra til å redusere problema ytterlegare.

Det eksisterer ikkje noko generelt krav om at samtykke skal vere skriftleg. Sidan det kan vere vanskeleg å vite kva dei registrerte har forstått og teke stilling til ved handlingane sine, kan det vere utfordrande å godtgjere at det er gitt eit implisitt samtykke.

Internasjonalt held ein fast ved at samtykke som grunnlag for behandling av personopplysningar skal vere klårt og tydeleg og innebere ein aktivitet frå den registrerte si side som stadfestar at vedkomande forstår at det vil bli behandla personopplysningar. Regjeringa meiner prinsippet om at samtykke helst skal vere ei uttrykkeleg erklæring eller aktiv handling, er eit godt prinsipp som det er viktig å halde fast ved også i tida framover.

5.1.4.2 Bindingar som påverkar samtykket

For at eit samtykke skal vere eit gyldig grunnlag for behandling av personopplysningar, er eit av krava at det må vere gitt frivillig. Frivillig inneber sjølvsagt at samtykket ikkje kan bli gitt under noka form for tvang. Men òg andre forhold kan påverke den frie viljen, til dømes at det er eit ujamt styrkeforhold mellom partane som inneber at den registrerte ikkje opplever å ha noko reelt val med omsyn til å gi samtykke. Dette kan blant anna vere tilfellet når innbyggjarane er i kontakt med offentlege styremakter. Nokre døme kan vise dei utfordringane den behandlingsansvarlege kan møte, og som kan tilseie at samtykke ikkje er eigna som grunnlag for behandling av personopplysningar.

Det blir i meldinga kapittel 6.4 vist til døme frå arbeidslivet og frå helse- og omsorgstjenesten.

5.1.4.3 Manglande samtykkekompetanse

Samtykkekompetansen til mindreårige

Mindreårige har i dei fleste tilfelle ikkje sjølvstendig samtykkekompetanse. Likevel er det mykje dei kan samtykkje i, avhengig av alder og mognad. Barnet sin alder og mognad vil vere eit viktig element i vurderinga av om barnet òg skal høyrast i spørsmålet om behandling av opplysningar.

For å tryggje barns personvern betre tilrådde Justis- og politidepartementet i Prop. 47 L (2011–2012) endringar i personopplysningslova § 11. Lovendringsforslaget vart vedteke, og frå 20. april 2012 følgjer det av personopplysningslova at ein ikkje kan behandle personopplysningar om barn i strid med det som er til beste for barnet. Prinsippet om barnet sitt beste tilseier at der barnet sitt behov for omsorg og vern i praksis ikkje fell saman med interessene til foreldra, må barnet sine interesser og behov gå føre. Dette gjeld òg for samtykke til behandling av personopplysningar.

Spørsmålet om samtykkekompetansen til mindreårige er særleg aktuelt ved behandling av personopplysningar i skule- og barnehagesektoren, i helse- og omsorgssektoren og i forskingssamanheng (sjå nærmare omtale i meldinga). Graden av sjølvråderett aukar med alderen. På dei nemnde områda er mindreårige sin samtykkekompetanse godt avklåra, og det er ikkje nødvendig med nye tiltak for å tryggje barna sitt personvern.

Det er særlege utfordringar knytte til innhenting av samtykke når mindreårige bruker tenester i informasjonssamfunnet. Barn og unge forstår i mindre grad enn vaksne kva opplysningar som blir lagra om dei, kva opplysningane blir brukte til, og kven som får tilgang til opplysningar dei gir frå seg når dei bruker ulike tenester på nett.

Samtykke til marknadsføring i sosiale medium, særleg kommersiell bruk av opplysningar om mindreårige

Bruk av sosiale medium og andre informasjonssamfunnstenester inneber i betydeleg grad eksponering for marknadsføring. Marknadsføringa er ofte spesielt retta mot brukaren ved å vere basert på analysar av nettaktivitetane til brukaren. Barn og unge har ofte vanskeleg for å forstå samanhengen mellom nettaktiviteten og reklamen dei blir eksponerte for.

Samtykke til at personopplysningar kan nyttast til marknadsføring på nett, blir ofte gitt på lite tydelege måtar. I 2005 utarbeidde Forbrukarombodet og Datatilsynet ei rettleiing om innhenting og bruk av barns personopplysningar. Sidan det har utviklinga i barns bruk av tenester i informasjonssamfunnet eksplodert.

På europeisk nivå blir det diskutert om det skal innførast ei aldersgrense for barns samtykkekompetanse i informasjonssamfunnet. Det er gjort framlegg om at føresette skal samtykkje så lenge barnet er under 13 år, og det skal leggjast til rette for at samtykket kan etterprøvast.

Det blir i meldinga peikt på at det er viktig å ha reglar som kan tryggje personvernet til norske barn på ein god måte, uavhengig av kva ein meiner er godt personvern i vertslandet for ulike sosiale nettsamfunn.

Det blir vidare vist til at det er viktig å følgje den internasjonale diskusjonen om korleis ein best kan tryggje barns personvern, både ved bruk av tenester i informasjonssamfunnet og elles, slik at landa kan stå samla i sine krav overfor tenestetilbydarane.

Samtykkeutfordringar når vaksne manglar samtykkekompetanse

Innhenting av samtykke til behandling av personopplysningar om personar med nedsett eller manglande vurderingsevne og især pasientar som lir av demens, reiser særlege utfordringar. Dette er derfor spesielt regulert i helse- og omsorgslovgivinga.

Bruken av velferdsteknologi har lenge vore eit aktuelt tema i helse- og omsorgssektoren. I rapporten frå Hagen-utvalet (NOU 2011:11 Innovasjon i omsorg) er det blant anna føreslått å innføre og vidareutvikle tryggingsalarmar som har funksjonar for lokalisering av brukaren. Dette er føreslått som ein del av eit nasjonalt program for velferdsteknologi. Utvalet gjer framlegg om å innføre særskild lovgiving knytt til formidling og bruk av varslings- og lokaliseringshjelpemiddel, medrekna behandling av personopplysningar som hjelpemidla genererer. Også frå anna hald, mellom anna Datatilsynet og Helsedirektoratet, har det vore etterlyst eit klårare regelverk om bruk av varslings- og lokaliseringsteknologi i tenesteytinga til pasientar og brukarar som manglar samtykkekompetanse.

Behandling av personopplysningar som kan følgje med bruk av slik teknologi, krev eit klårt rettsgrunnlag etter personopplysningslova, helst i form av samtykke frå den registrerte (pasienten eller brukaren). Pasientane eller brukarane må ha samtykkekompetanse.

Regjeringa ønskjer å skape rettsleg klårleik og leggje betre til rette for teknologi som kan gi kvar einskild betre høve til utfalding og livskvalitet samstundes som han eller ho får oppfylt behovet for tryggleik. Regjeringa har derfor sendt eit framlegg om lovendring på dette området på høyring. Framlegget gir helse- og omsorgstenesta høve til å ta i bruk varslings- og lokaliseringssystem for demente og andre som manglar samtykkekompetanse.

5.1.4.4 Gir samtykke alltid godt personvern?

Det blir i meldinga peikt på at samtykke som behandlingsgrunnlag er eit viktig element i det å ha råderett over eigne personopplysningar. Råderetten står sentralt i både norske personvernreglar og i EUs arbeid med revisjon av personvernregelverket. I forslaget til revidert regelverk er det tydelegare fokus på reelt samtykke til behandling av personopplysningar. Ein fordel med samtykke som behandlingsgrunnlag er at det stør opp under og legg grunnlag for bruken av mange av dei andre rettane innbyggjarane har i samband med behandling av personopplysningar.

I meldinga blir det peikt på at det likevel er grunn til å spørje om samtykke alltid gir godt personvern. I 2005 gjennomførte Transportøkonomisk institutt ei stor undersøking om folks haldningar til og kunnskap om personvern på oppdrag frå Moderniseringsdepartementet og Datatilsynet. Undersøkinga viste at nordmenn flest reflekterer lite over eige personvern. Samstundes viser undersøkinga at befolkninga har tillit til at innsamla personopplysningar blir behandla på ein god måte både i offentleg og privat verksemd.

Ut frå svar i undersøkinga er det grunn til å rekne med at mange samtykkjer i behandling av personopplysningar utan å lese informasjonen dei får i samband med samtykkeerklæringa.

Verdien av samtykke som behandlingsgrunnlag har vore framheva og understreka dei siste åra, både nasjonalt og internasjonalt. Samtykke som behandlingsgrunnlag kan likevel gi eit inntrykk av ein råderett som kanskje ikkje er reell. Ein bør derfor vurdere nøye om ei personopplysningsbehandling eignar seg for å vere samtykkebasert.

Det er avgjerande at befolkninga blir sett i stand til å ta vare på sitt eige personvern. Samtykke er viktig i denne samanhengen og kan vanskeleg bli erstatta av andre ordningar.

5.1.5 Reservasjonsrett

Reservasjonsrett kan vere aktuelt der føremålet med eit tiltak ikkje blir oppnådd med bruk av samtykke og ein vurderer at nytta av personopplysningsbehandlinga er vesentleg større enn personvernulempa for dei registrerte. Reservasjonsrett blir mellom anna brukt ved etablering av Nasjonal kjernejournal. Registrering av opplysningar i Nasjonal kjernejournal er lovheimla, men samstundes frivillig ved at kvar einskild pasient har rett til å reservere seg mot

å vere med. Seinare uthenting av opplysningar om einskildpasientar frå kjernejournalen er basert på samtykke får pasienten, med unntak av nokre situasjonar, typisk i ein akuttmedisinsk situasjon.

I nokre samanhengar kan reservasjonsrett for den einskilde i kombinasjon med lovheimel som behandlingsgrunnlag òg gi ei oppleving av større valfridom enn registrering med grunnlag i samtykke. Dette gjeld mellom anna der den registrerte på ein eller annan måte er avhengig av tenester frå den behandlingsansvarlege, for eksempel i pasient-lege-relasjonar. I nokre situasjonar kan derfor reservasjonsrett gi godt personvern for den einskilde.

For at dei registrerte skal kunne vurdere om dei ønskjer å reservere seg mot innsamling og bruk av personopplysningar, må dei få informasjon om alle delar av bruken slik at dei blir i stand til å ta eit slikt val. Informasjonen som skal gi grunnlag for å vurdere bruk av reservasjonsretten, bør i det vesentlege vere den same som om behandlinga skulle bli basert på samtykke frå dei registrerte. Det at ein på opplyst grunnlag vel å la vere å reservere seg, er likevel ikkje det same som å samtykkje. Det å gjere noko aktivt er alltid meir krevjande enn passivitet, og ein må gå ut frå at terskelen for å reservere seg er høgare enn for berre stillteiande å akseptere noko. Dermed kan ei løysing med reservasjonsrett ikkje likestillast med ei samtykkeløysing, der den registrerte blir tvinga til aktivt å ta stilling til behandling av personopplysningar.

Det at ein kan reservere seg mot ei behandling av personopplysningar, tek ikkje vare på alle dei same omsyna som det er meininga at samtykkekrava skal tryggje. Reservasjonsrett åleine kan derfor ikkje nyttast som eit behandlingsgrunnlag etter personopplysningsregelverket. Det blir gjerne gitt tilbod om reservasjonsrett fordi ein trur at dei registrerte kan reagere på personopplysningsbehandlinga, og at det derfor er fornuftig å opne for at dei som ikkje ønskjer å ta del i behandlinga, kan sleppe det. Grunnlaget kan vere varetaking av den rettkomne interessa den behandlingsansvarlege har i å behandle personopplysningar etter personopplysningslova § 8 bokstav c eller ein annan særskild lovheimel. Reservasjonsretten er ikkje eit behandlingsgrunnlag etter personopplysningslova, men kan vere eit personvernfremjande tiltak. Det er viktig å halde fast ved at reservasjonsrett ikkje er det same som at bruk av personopplysningar har grunnlag i samtykke. Regjeringa meiner likevel at reservasjonsrett i mange samanhengar vil gi godt personvern samstundes som det legg til rette for god ivaretaking av allmenne interesser. Dette kan gi grunnlag for å vurdere reservasjonsrett i fleire samanhengar enn det som i dag er tilfellet.

5.1.6 Hovudpunkt kapittel

- Dei registrerte skal i størst mogleg grad ha råderett over eigne personopplysningar.
- Det offentlege si behandling av personopplysningar bør ha heimel i lov eller vere grunngitt i at det er nødvendig for utøving av offentleg myndigheit eller utføring av lovpålagde oppgåver.
- I privat verksemd er samtykke det føretrekte behandlingsgrunnlaget der den registrerte har eit reelt val om å la seg registrere.
- I somme samanhengar kan lovheimel for behandling av personopplysningar saman med ein reservasjonsrett for dei registrerte gi den mest reelle råderetten for den einskilde.

5.2 Komiteens merknader

Komiteen er kjent med at personopplysningsloven (Pol.) både angir samtykke og en såkalt nødvendiggjørende grunn som rettslig grunnlag for å behandle personopplysninger.

Likeledes er komiteen av den oppfatning at man alltid skal vurdere om samtykke er et realistisk behandlingsgrunnlag. Prinsippet er at den registrerte i størst mulig grad skal ha råderetten over egne personopplysninger.

Komiteens medlemmer fra Fremskrittspartiet, Høyre og Kristelig Folkeparti sier seg uenig i regjeringens vurdering av at «samtykke er lite egnet for de fleste behandlinger av personopplysninger». Disse medlemmer vil tvert imot hevde at informert, reelt samtykke er det foretrukne behandlingsgrunnlag for innhenting av personopplysninger, og at de praktiske ulemper ved samtykke er sterkt overdrevet. Disse medlemmer vil også fremheve reservasjonsrett som et alternativ til lovhjemlet masseinnhenting uten samtykke, men ikke som alternativ til samtykke der det er praktisk forsvarlig.

Disse medlemmer vil også fremheve at selv om innhenting av samtykke kan være mer omstendelig enn automatisk registrering, vil den registrerte få en sterkere bevissthet om sin råderett over egne opplysninger, og at man også kan bevisstgjøre den registrerte om at opplysninger som innhentes i forbindelse med søknad om ytelser, også kan bli gjenstand for kontroll, og dermed være forebyggende mot uriktige opplysninger.

Disse medlemmer viser til at samtykke er det grunnleggende behandlingsgrunnlag når private, for eksempel næringslivet, registrerer opplysninger, men deler ikke regjeringens oppfatning om at kontaktinformasjon i seg selv er lite inngripende. Ved sammenkobling av andre opplysninger man har fått gjennom kundeforholdet, og ved utveksling av kontaktinformasjon med andre, vil bildet kunne bli et

annet. Likeledes tilsier respekt for den enkelte at man gis en reell reservasjonsrett mot markedsføring man ikke ønsker.

6. Personvernrettar og -plikter

6.1 Sammendrag

For å sikre ivaretaking av personvernomsyn har den registrerte fått ein del rettar. Dessutan er dei behandlingsansvarlege pålagde ein del plikter som skal bidra til at personvernet til dei registrerte blir teke hand om.

Ein del personvernrettar er òg nedfelte i anna regelverk, og dette regelverket kan i praksis ha meir å seie enn personopplysningslova. For mange er det truleg reglane i forvaltningslova som ligg til grunn for krav om innsyn i personopplysningar i forvaltninga, og ikkje innsynsreglane i personopplysningslova. I privat sektor er det derimot innsynsreglane i personopplysningslova som gir grunnlag for innsyn. Teiepliktsreglar, som det er mange av i norsk rett, er òg reglar som bidreg til å tryggje personvernet til dei registrerte.

Mange av rettane i personopplysningsregelverket er relativt lite kjende, og regjeringa meiner det er nødvendig å vurdere tiltak som kan bidra til at rettane blir både betre kjende og betre nytta.

6.1.1 Brukarmedverking og kontroll over eigne personopplysningar

Personvern er både ein kollektiv og ein individuell rett. Det finst ei rekkje reglar som skal bidra til å gi brukarane auka kontroll og råderett over eigne personopplysningar, blant anna reglar om innsyn, reservasjonsrett, retting og sletting og om retten til å bli gløymd. Ein må bruke handlingsrommet reglane gir på ein god måte.

6.1.1.1 Kontroll over eigne personopplysningar

Sjølvråderett er eit grunnleggjande prinsipp i norsk rett. I personvernsamanheng vil sjølvråderetten seie at individet i stor grad har rett til å bestemme over sine eigne personopplysningar når desse kan samlast inn, og kva dei kan brukast til.

Ei anna side ved sjølvråderetten er at individet skal kunne utøve ein viss grad av kontroll med flyten og bruken av personopplysningane sine, også når dei er komne i andre sine hender.

Personopplysningar har i lang tid vore ei vare og samstundes eit betalingsmiddel. Mange gir frå seg personopplysningar i byte mot andre gode. Viljen næringslivet har til å betale for personopplysningar, er relativt liten, samstundes som verdien personopplysningar har for dei i kommersiell samanheng, synest høg. I enkelte verksemder kan eit godt utvikla kunderegister vere den viktigaste verdien i selskapet. Informasjonen om brukarane har enorm forretningsverdi. Utan all informasjonen kvar enkelt brukar legg ut, har for eksempel dei sosiale nettstadene liten kommersiell verdi. Det er derfor rimeleg at innbyggjarane i det minste har ein viss råderett over den verdien kvar enkelt representerer. Dersom brukaren ikkje lenger ønskjer å vere brukar av ein sosial nettstad, og ikkje lenger tek imot noka vare, bør han følgjeleg kunne krevje at betalinga for tenesta sluttar i den forstand at personopplysningane blir sletta eller leverte tilbake.

Kontroll over eigne personopplysningar krev informasjon og kunnskap. Retten til informasjon og retten til innsyn er derfor grunnleggjande i personvernsamanheng.

6.1.1.2 Rett til anonymitet

I mange daglege gjeremål lèt innbyggjarane etter seg informasjon som gir høve til personidentifisering. Ulike automatiserte registrerings- og betalingssystem forenklar kvardagen både for tenesteytaren og -mottakaren. Personidentifiserbar informasjon frå registreringsordningane kan likevel seie mykje om rørslene og åtferda til dei registrerte.

Med omgrepet anonymitet forstår ein normalt at identiteten ikkje er kjend. Men retten til å opptre og ferdast anonymt er ikkje uttrykkeleg fastslått i norsk rett. Denne retten kan likevel til ein viss grad tolkast av prinsippet om dataminimalitet. Er identifikasjon ikkje nødvendig, skal dei registrerte ha høve til å opptre anonymt.

Retten til anonymitet er ein rett med modifikasjonar. Dette gjeld ikkje minst i transportsektoren. Det finst både internasjonale og norske reglar som avgrensar retten den enkelte har til å reise utan å måtte gi frå seg personopplysningar.

Også i alminneleg varehandel er anonymiteten på vikande front.

Utviklinga går i retning av stadig fleire løysingar som gjer det mogleg å identifisere personar. Det er likevel sjeldan ein tek seg tid til å diskutere dei utfordringane som følgjer med ei utvikling der heilt daglegdagse aktivitetar lèt etter seg spor som både politi, andre styremakter, næringsdrivande og kriminelle, lovleg eller ulovleg, kan skaffe seg tilgang til. Utviklinga viser at det er behov for ein overordna debatt om retten til anonymitet, slik at ein kan sjå utfordringar i ulike sektorar i samanheng. Når ein greier ut ulike tiltak som har eller kan ha personvernkonsekvensar, bør prinsippet om dataminimalitet ha betydeleg vekt. Ein skal vurdere om det er mogleg å bruke anonyme alternativ. Dei elektroniske reisekorta i kollektivtrafikken er eit eksempel på eit områ-

de der retten til anonymitet er teken hand om på ein god måte.

6.1.1.3 Retten til å bli gløymd

I forlenginga av retten til anonymitet snakkar ein stadig oftare om retten til å bli gløymd. EU-kommisjonen har sett fokus på retten til å vere anonym gjennom å føreslå ein rett til å bli gløymd («right to be forgotten») i utkastet til revidert personvernregelverk. Retten til å bli gløymd vil særleg kunne gi grunn til sletting av opplysningar som er lagde ut på nett.

Langt på veg vil ein rett til å bli gløymd falle saman med dei tradisjonelle norske reglane om rett til å få sletta opplysningar som ikkje lenger er nødvendige for behandlingsføremålet. EU-forslaget til reglar om retten til å bli gløymd femner likevel vidare. Forslaget går ut på at den registrerte òg kan krevje at den behandlingsansvarlege set i verk tiltak for å få sletta kopiar av informasjon som er spreidd på Internett. Det same gjeld lenkjer til informasjonen som den registrerte ønskjer å få sletta. Forslaget står òg fram som eit særleg vern av barn, som ikkje alltid er like kritiske til kva informasjon dei publiserer.

Forslaget har likevel møtt kritikk frå dei som meiner ein slik regel vil gi folk høve til å redigere liva sine ut over det som synest rimeleg. Omsynet til dokumentasjon for ettertida kan derfor tale mot ein rett til å redigere ettermælet sitt på den måten som retten til å bli gløymd kan synast å opne for.

For å gi den enkelte størst mogleg kontroll med bruken av opplysningar om seg sjølv kan det vere ei løysing å gi den registrerte rett til å flytte informasjon frå ein tenestetilbydar til ein annan.

Eit anna og meir krevjande element ved retten til å bli gløymd er ein eventuell rett til å få sletta opplysningar som er distribuerte av andre på nett. Her er forholdet til ytringsfridomen eit sentralt vurderingstema. Eit spørsmål er òg kva opplysningar det er praktisk mogleg å få sletta.

Dersom ein rett til å bli gløymd skal få reell verdi, må han vere mogleg å praktisere. Dette krev blant anna internasjonal semje om eit slikt prinsipp. Noreg kan ikkje åleine innføre ein regel som ville få så mykje å seie for internasjonal samhandling. Ein rett til å bli gløymd må i det minste baserast på europeisk semje. Regjeringa vil følgje debatten om retten til å bli gløymd og den internasjonale utviklinga på dette området i tida framover og sjå i kva lei ho går, når det eventuelt blir aktuelt å vurdere norske reglar på området.

6.1.2 Den behandlingsansvarlege

Etter personopplysningslova er det den behandlingsansvarlege som avgjer føremålet med ei personopplysningsbehandling, og kva hjelpemiddel som skal nyttast. Den behandlingsansvarlege har ansvar for å oppfylle alle plikter etter personopplysningslova. Dette inneber at den behandlingsansvarlege har ansvar for at det finst rutinar og system for å leve opp til personopplysningsregelverket og tryggje rettane til dei registrerte etter regelverket.

Det er ei generell utfordring at personvernregelverket er lite kjent blant dei som behandlar personopplysningar. Det blir i meldinga vist til resultata frå ei undersøking som Trafikkøkonomisk institutt (TØI) gjorde av behandlinga av personopplysningar i norske verksemder i 2005. Nettopp på bakgrunn av desse resultata har regjeringa over fleire år gitt øyremerkte midlar til Datatilsynet for arbeid med å gjere regelverket om informasjonstryggleik betre kjent blant dei behandlingsansvarlege. Datatilsynet si satsing på opplæring av personvernombod er òg eit tiltak for å gjere regelverket betre kjent blant behandlingsansvarlege. Det kan vere føremålstenleg å gjennomføre ei ny personvernundersøking.

Trygginga av personvernrettane er nært knytt til pliktene den behandlingsansvarlege har, og korleis vedkomande oppfyller dei. Både reglane som heimlar rettane og reglane om pliktene er, til ein viss grad skjønsprega, og gir eit visst handlingsrom. Regjeringa har som mål å bruke dette rommet på ein måte som gagnar både den behandlingsansvarlege og dei registrerte.

6.1.3 Plikt til å klårgjere personvernkonsekvensar

Ei vurdering av personvernkonsekvensar vil leggje grunnlag for tiltak som skal ta hand om personvernrettane til dei registrerte på best mogleg måte.

Ein analyse av personvernkonsekvensar kan vise at det er fleire konkurrerande eller motstridande personvernomsyn å ta hand om i ei sak. Då må ein vurdere kva personverninteresse som skal vege tyngst. Analyse av personvernkonsekvensar vil òg kunne vise at personvernomsyn står mot andre samfunnsomsyn eller private omsyn.

Det er som regel rimelegare å leggje til rette for ivaretaking av personvern når eit system blir utvikla, enn å omarbeide eit eksisterande system slik at det kan ta omsyn til personverninteresser. Dette tilseier at det vil vere i den behandlingsansvarlege si interesse å leggje til rette for god ivaretaking av personvernet til dei registrerte så tidleg som mogleg i arbeidet med nye system.

Dersom personvernkonsekvensar er godt klårgjorde og drøfta ved førebuing av nye lovreglar, blir personvernkonsekvensar synlege for Stortinget. Dette vil gi Stortinget grunnlag for å ta stilling til personvernkonsekvensane i samband med vedtaking av lovreglane. Rettleiinga om vurdering av personvernkonsekvensar som Fornyings- og administrasjonsde-

partementet har laga, er ei støtte til statlege etatar slik at dei på ein god måte kan klårgjere personvernkonsekvensar ved planlagde tiltak. Trass i at rettleiinga har eksistert i nokre år, er det framleis for mange offentlege utgreiingar som manglar gode drøftingar av personvern. Det vil bli vurdert tiltak for å sikre at saksbehandlarar i offentlege verksemder kjenner og bruker rettleiinga.

Sjølv om den omtala rettleiinga er utarbeidd for statlege etatar, er råda i rettleiinga allmenngyldige. Rettleiinga kan derfor vere nyttig også utanfor det statlege forvaltningsområdet. For å styrkje ivaretakinga av personvernet til dei registrerte er det i regelverksrevisjonen i EU føreslått å regelfeste ei plikt til å gjennomføre ein såkalla «data protection impact assessment».

Utgreiing av personvernkonsekvensar og gjennomføring av personvernanalysar bør vere eit naturleg ledd i tilrettelegginga for behandling av personopplysningar både i privat og offentleg sektor. Dette kan ein blant anna oppnå gjennom samarbeid med næringslivet og næringslivsorganisasjonane. Informasjon om personvernanalysar og personvernregelverket kan følgje med annan informasjon som blir gitt til næringsdrivande ved oppstart av næringsverksemd. Nettsidene til Brønnøysundregistra kan vere ein veleigna informasjonsstad. I tillegg er nettsidene til Datatilsynet ein naturleg informasjonsstad.

6.1.4 Plikt til å gi informasjon om behandling av personopplysningar

6.1.4.1 Eksisterande informasjonsplikter

Dei registrerte har omfattande krav på informasjon frå den behandlingsansvarlege om pågåande personopplysningsbehandlingar, både ved direkte førespurnad og på initiativ frå den behandlingsansvarlege. Informasjon er viktig for at dei registrerte skal kunne nytte dei andre rettane sine etter lova. Informasjonsplikta står derfor sentralt.

Regelverket pålegg den behandlingsansvarlege ei plikt til å ha tilgjengeleg generell informasjon om behandling av personopplysningar for dei som spør om det, uansett om spørjaren er registrert eller ikkje. I tillegg har alle registrerte rett til innsyn i dei opplysningane som er lagra om dei, og dessutan ein del informasjon om korleis opplysningane blir behandla. Denne informasjonen skal den behandlingsansvarlege gi på ein klår og tydeleg måte som set den registrerte i stand til å ta hand om interessene sine.

For tre spesielle typar personopplysningsbehandlingar er det særskilde informasjonsreglar. Dette gjeld ved bruk av personprofilar, ved automatiserte avgjerder og i kredittopplysningsverksemd. Desse er omtala nærmare i meldinga punkt 7.4.1.

6.1.4.2 Etterleving av informasjonsreglane

Det blir i meldinga peikt på at det for å setje innbyggjarane betre i stand til å ta hand om sitt eige personvern, er nødvendig å skape større medvit om informasjonsplikta som kviler på den behandlingsansvarlege. Dette kan blant anna gjerast gjennom informasjon på offentlege nettstader som blir brukte av næringslivet, til dømes nettsidene til Brønnøysundregistra. På nettsidene til Datatilsynet finn ein denne typen informasjon under overskrifta personvernerklæring. Både offentlege og private behandlingsansvarlege bør sørgje for å ha slik informasjon lett tilgjengeleg på nettsidene sine, for eksempel under overskrifta personverninformasjon eller personvernerklæring. For å hjelpe dei behandlingsansvarlege til å oppfylle informasjonspliktene sine vil regjeringa utarbeide ein mal for denne typen informasjon.

Det vil vere praktisk for dei registrerte å kunne hente informasjon om behandling av personopplysningar elektronisk når det passar for dei, utan å vere avhengige av opningstider og tilgjengelege kundebehandlarar.

Det finst gode eksempel på verksemder som har gjennomarbeidd og lett tilgjengeleg informasjon om behandling av personopplysningar på nettsidene sine. Saman med informasjonen får ein ofte høve til å logge seg inn på personlege informasjonssider som gir tilgang til noko av den informasjonen verksemda har lagra om den enkelte. Som ledd i regjeringa sitt arbeid med digitalisering av offentleg sektor kan auka bruk av elektroniske innsynsløysingar for å gi den enkelte betre kontroll med eigne opplysningar vere aktuelt. Avgjerande for bruk av automatiserte innsynsløysingar er likevel at ein kan ta hand om informasjonstryggleiken på ein god måte, slik at dei registrerte har tillit til løysingane.

Samstundes kan det vere grunn til å sjå nærmare på bruk av gjenpartsplikt, det vil seie automatisk varsling ved innsyn i eller utlevering av personopplysningar. Regjeringa legg til grunn at elektronisk gjenpartsplikt kan vere ein praktisk måte å gjennomføre innsynsrett på i mange samanhengar. Samstundes må ein ikkje bruke ordninga på ein måte som medfører at dei registrerte druknar i informasjon. Samstundes som elektronisk gjenpartsplikt kan vere ei god løysing for å gi informasjon til dei registrerte, kan det gjere dei behandlingsansvarlege meir medvitne. Det offentlege bør vere ein pådrivar for bruk av løysingar for utsending av elektronisk gjenpart til dei registrerte i samanhengar der dette er naturleg.

I april 2012 tok endringane i personopplysningslova § 11 til å gjelde. Endringane understrekar at personopplysningar som gjeld barn, ikkje kan behandlast på ein måte som er uforsvarleg av omsyn til barnet sitt beste. God og forståeleg informasjon retta mot barn og unge kan vere eit ledd i etterlevinga av

desse reglane. For det offentlege vil det særleg vere aktuelt å sørgje for god og tilpassa informasjon til elevane om korleis skulen behandlar personopplysningar om dei. Det finst allereie informasjon på området utarbeidd av Senter for IKT i utdanninga.

6.1.4.3 EUs forslag til forsterka informasjonsplikt

I EUs forordningsforslag er det gjort framlegg om både generell informasjonsplikt og konkret innsynsrett for dei registrerte. Forståeleg og lett tilgjengeleg informasjon om behandling av personopplysningar og om rettane til dei registrerte er framheva. Det blir særleg understreka at informasjonen skal vere tilpassa mottakaren, spesielt dersom mottakaren er mindreårig.

EU framhevar òg verdien av at den behandlingsansvarlege etablerer rutinar som gjer at rettane til den registrerte blir oppfylte på ein korrekt måte innan rimeleg tid. Dersom den behandlingsansvarlege nektar å etterkome informasjonskrav, skal den registrerte få ei grunngiving og informasjon om klageretten.

6.1.5 Lagringstid

6.1.5.1 Innleiing

Prinsippet om dataminimalitet tilseier at opplysningar ikkje blir lagra lenger enn nødvendig for det føremålet dei er innsamla for. Personopplysningslova inneheld likevel ingen reglar om maksimal oppbevaringstid eller slettefrist for personopplysningar. Ein generell sletteregel ville det vere vanskeleg å praktisere, og truleg ville han føre til at informasjon vart lagra lenger enn nødvendig fordi slettefristen vart sedd på som ei opning for å behalde data inntil maksimal lagringstid var oppnådd. Det er sjeldan reglar om behandling av personopplysningar har klåre og absolutte fristar for sletting av personopplysningar. Andre lovreglar har derimot heilt konkrete slettereglar, og dei vil gå føre dei generelle slettereglane i personopplysningslova.

6.1.5.2 Etterleving av slettereglar i personopplysningsregelverket

I tillegg til kravet om at det skal vere sakleg behov for dei personopplysningane som blir behandla, pålegg personopplysningslova den behandlingsansvarlege ei plikt til å slette opplysningar som er unødvendige. Ein må vurdere sletting opp mot eventuelle krav om vidare lagring i for eksempel arkivregelverket i offentleg sektor, bokføringsregelverket eller anna spesialregelverk. Deretter må ein etablere rutinar for sletting av opplysningar som det ikkje lenger er sakleg behov for i verksemda.

Det kan vere meir ressurskrevjande å etablere rutinar for sletting enn det er å lagre alt som er generert eller på annan måte innsamla.

Det kan vere føremålstenleg å ta i bruk teknologi for å leggje til rette for betre etterleving av slettereglar i personopplysningsregelverket. Automatiserte slette- eller arkivrutinar kan bidra til betre regeletterleving og dermed betre personvern. Dersom det er juridisk mogleg, kan ein implementere automatiserte sletterutinar. I offentleg sektor vil arkivregelverket setje grenser for høvet til å slette opplysningar.

Skal automatiserte slette- og arkiveringsrutinar fungere, krevst det grundige vurderingar når dei blir etablerte. Der spesialregelverk ikkje er til hinder for det, bør ein alltid vurdere tilrettelegging for automatiserte slette- og arkiveringsrutinar når nye IKT-system for behandling av personopplysningar blir utvikla. Når nye tiltak og system med personvernkonsekvensar blir utgreidde, bør ein òg vurdere bruk av teknologi som reduserer mengda av overskotsinformasjon. Personvernfremjande bruk av teknologi kan på denne måten medverke til at personvernet blir tryggja på ein betre måte.

6.1.6 Internkontroll

Det blir i meldinga peikt på at eit godt internkontrollsystem kan vere avgjerande for å sikre forsvarleg behandling av personopplysningar. Personopplysningsregelverket pålegg den behandlingsansvarlege å etablere internkontroll på personvernområdet.

Verksemder som kjem inn under personopplysningsregelverket, må setje i verk og dokumentere systematiske tiltak for å sørgje for etterleving av plikter etter personvernreglane. Den behandlingsansvarlege skal gjennomføre ei risikovurdering som grunnlag for iverksetjing av tiltak for informasjonstryggleik. Det finst i dag inga plikt til å gjennomføre risikovurderingar i arbeidet med internkontroll på dei andre områda i lova. Erfaring tilseier at mange behandlingsansvarlege ikkje gjennomfører risikovurderingar, og konsekvensen er ofte mangelfull internkontroll.

God internkontroll er uttrykk for ei bevisst haldning til og bevisste val om personvern. Tilsynsverksemda til Datatilsynet avdekkjer likevel at mange verksemder har liten kunnskap om personvernregelverket og dei pliktene som følgjer med det å behandle personopplysningar. Derfor er det viktig å setje i verk tiltak for å betre kjennskapen til og etterlevinga av internkontrollreglane på personvernområdet. I perioden 2009–2011 styrkte regjeringa budsjettet til Datatilsynet med betydelege midlar for å få gjennomført eit prosjekt om internkontroll i små og mellomstore verksemder. I dette arbeidet vart det blant anna satsa på opplæring av personvernombod.

Datatilsynet har utarbeidd omfattande kunnskaps- og rettleiingsmateriell, medrekna opplæringsprogram om internkontroll og informasjonstryggleik som blant anna er tilgjengelege på nettsidene til etaten.

Internkontroll på personvernområdet bør bli like naturleg for alle som behandlar personopplysningar, som internkontroll på HMS-området er for alle arbeidsgivarar. Som ei vidareføring av rettleiinga Vurdering av personvernkonsekvenser, som vart utarbeidd av Fornyings- og administrasjonsdepartementet i 2008, vil regjeringa derfor utarbeide rettleiingsmateriell om korleis internkontrollplikta kan etterlevast på personvernområdet i offentleg verksemd.

6.1.6.1 Handtering og rapportering av regelbrot

Uansett kor god informasjonstryggleik og uansett kor gode system for regeletterleving ein behandlingsansvarleg har, kan regelbrot skje. Enkelte regelbrot vil vere meir alvorlege og kan få større konsekvensar enn andre. For ein del slike tilfelle inneheld personopplysningsforskrifta reglar om avviksrapportering. Dersom brot på reglar og rutinar fører til at uvedkomande får tilgang til personopplysningar som er konfidensielle, skal den behandlingsansvarlege melde dette til Datatilsynet. Rutinar for retting av slike avvik og rapportering til Datatilsynet bør vere ein naturleg del av eit internkontrollsystem.

Ei rekkje tryggleiksbrot blir aldri rapporterte til Datatilsynet. Det er nødvendig å rette merksemd mot etterleving av dei gjeldande rapporteringsreglane som ledd i arbeidet med å betre etterlevinga av internkontrollreglane. I arbeidet med å leggje til rette informasjon om internkontroll for offentleg verksemd vil regjeringa òg leggje vekt på verdien av rapportering til personvernstyremakta som ledd i avvikshandteringa.

6.1.7 Hovudpunkt kapittel

- Innbyggjarane skal ha størst mogleg råderett over eigne personopplysningar og må få tilpassa informasjon frå dei behandlingsansvarlege. Det vil bli utarbeidd ein rettleiar om plikta til å gi informasjon om behandling av personopplysningar.
- Elektroniske løysingar for innsyn bør vurderast dersom ein samstundes kan ta hand om informasjonstryggleiken i systema.
- Elektronisk gjenpart som informasjonskjelde bør vurderast ved oppretting av store personregister som skal vere tilgjengelege for mange brukarar.
- Dataminimalitet er eit mål, og det skal leggjast til rette for sporfrie alternativ og bruk av teknologi for å redusere mengda av overskotsinformasjon der dette er praktisk mogleg.
- Arbeidet for å gjere personvernreglane kjende må halde fram.
- Dei behandlingsansvarlege skal prioritere utgreiing av personvernkonsekvensar og tilrettelegging av internkontroll. Det vil bli utarbeidd ein rettleiar om internkontroll etter personopplysningslova.

6.2 Komiteens merknader

Komiteen vil fremheve prinsippet om dataminimalitet, dvs. at det ikke registreres flere opplysninger enn det som er nødvendig for formålet. For øvrig bør publikum tilbys anonyme eller pseudonyme løsninger.

Komiteen har også merket seg at EU-kommisjonen i tråd med tidligere initiativ vil vektlegge prinsippet om å kunne bli glemt, dvs. en generell regel om å kunne trekke tilbake samtykke. I praksis vil en slik regel være svært viktig for barn og unge.

Komiteen ser positivt på at en bedrift også får pålegg om å organisere personvernspørsmål og etterlevelsen av regelverket, jf. pol. § 14.

Komiteens medlemmer fra Høyre og Kristelig Folkeparti hilser velkommen bestemmelsene i EUs foreslåtte forordning om personvern som går ut på å gi den enkelte forsterket informasjonsrett og konkret mulighet til innsyn i hva som er registrert av opplysninger om vedkommende.

7. Sosiale medium og personvern

7.1 Sammendrag

7.1.1 Innleiing

I rapporten sin tek Personvernkommisjonen opp tilhøvet mellom personvernet og media og personvernet for barn og unge. Kommisjonen fremjar fleire forslag til tiltak på desse to områda, til dømes å vedta ei eiga medieansvarslov som blant anna skal regulere redaktøransvar for alle medium, å utvide ordninga med fritt rettsråd til å omfatte visse saker mot media, og å etablere eit organ for nettytringar, slettehjelp og styrking av personvernet ved bruk av digitale medium.

Etter at Personvernkommisjonen leverte rapporten sin i 2009, er sosiale medium og personvern drøfta av Medieansvarsutvalet (NOU 2011:12 Ytringsfridom og ansvar i ein ny mediekvardag), medan personvernutfordringar for barn og unge ved bruk av sosiale medium er drøfta nærmare i NOU 2011:20 Ungdom, makt og medverking, kapittel 8.

Det blir i meldinga vist til at tilbydarane av sosiale medium får tilgang til store mengder av personopplysningar, og brukarane har liten eller ingen kontroll over korleis tilbydarane bruker opplysningane.

Stadig fleire opprettar profilar på ulike sosiale nettverk – både privatpersonar, offentlege personar, kommersielle aktørar og offentlege verksemder. Facebook er det største sosiale nettverket i verda, med om lag 800 millionar brukarar. Det finst uendeleg mange andre sosiale nettverk som nordmenn bruker dagleg.

Barn og unge er hyppige brukarar av sosiale medium. Ei «trygg bruk»-undersøking frå Medietilsynet frå 2010 Fakta om barn og unges bruk og opplevelse av digitale medier viser at barn og unge startar tidlegare med digitale medium no enn dei gjorde i 2008.

Barn har fått eit særskilt internasjonalt vern gjennom FNs barnekonvensjon artikkel 16.

7.1.2 Skiljet mellom redigerte massemedium og andre elektroniske tenester, medrekna sosiale medium

Dei redigerte media fyller ein særleg demokratisk funksjon som kjelder til nyhende og som plattform for den offentlege samfunnsdebatten. Sosiale medium, bloggar og andre brukargenererte elektroniske tenester kan innanfor avgrensa brukargrupper eller tema fylle noko av den same funksjonen, men vil normalt mangle den breidda i innhald og nedslagsfelt som gir dei redigerte massemedia ei særleg stilling. Dei vil òg mangle det bransjeetiske grunnlaget og dei journalistiske profesjonsnormene som ligg til grunn for verksemda til massemedia.

Skiljet mellom redigerte og ikkje-redigerte medium er relevant i diskusjonen av personvernspørsmål.

Den vidare omtala i dette kapitlet er avgrensa til særlege problemstillingar knytte til utviklinga av sosiale medium.

7.1.3 Særtrekk ved sosiale medium

Eit særtrekk ved sosiale medium er at kvar einskild brukar kan publisere informasjon for ein vid krins utan å vere under kontroll av ein redaktør og utan å ha profesjonell erfaring eller etiske normer å rette seg etter.

Fleire ulike variantar av sosiale medium har fått fotfeste og er utbreidde over heile verda. Dei sosiale media, som Facebook, Twitter og YouTube, er ikkje lenger berre ungdomsfenomen, men blir brukte av stadig større delar av befolkninga. Likevel er mange av dei utfordringane som følgjer med det å eksponere seg på nett, særleg aktuelle for barn og unge, fordi barn ikkje har dei nødvendige føresetnadene for å forstå korleis personopplysningar blir behandla, og konsekvensane av det. Samstundes er det ein aukande tendens til at vaksne legg ut informasjon og bilete av barna sine på nett utan å vurdere konsekvensane for barna eller spørje barna om dei synest slik eksponering er greitt. Ein generell konsekvens av den auka nettbruken er at brukarane oftare opplever å få personvernet sitt krenkt på nett. Dei fleste veit i realiteten lite om kva som blir lagt igjen av informasjon på nettet.

7.1.4 Utanlandske tilbydarar av sosiale medium

Den norske marknaden for sosiale medium er i dag dominert av utanlandske tenestetilbydarar.

For ein norsk nettbrukar treng ikkje nasjonaliteten til ei teneste ha noko å seie. Erfaringa har vist at det er først når brukaren ønskjer å kontakte tenestetilbydaren, at nasjonalitet kan spele inn. Sjølv om det kan vere like vanskeleg å kome i kontakt med ein norsk tilbydar som med ein utanlandsk, vil det alltid vere lettare å spore opp ansvarssubjekta bak eit norsk sosialt medium. Juridisk har nasjonaliteten til ein tilbydar derimot meir å seie. Jamvel om Internett i seg sjølv er globalt, er lovgivinga som regulerer nettet, først og fremst nasjonal.

7.1.5 Generelle personvernutfordringar ved bruk av sosiale medium

7.1.5.1 Openheit og transparens

Det blir i meldinga vist til at ei overordna utfordring med mange sosiale medium er manglande openheit og transparens. Sjølv om dei fleste tenestetilbydarar krev samtykke til dei vilkåra tenesta har fastsett, gir innhaldet i desse vilkåra ofte ikkje svar på kva opplysningar som blir behandla, kva som er føremålet med behandlingane, korleis opplysningane blir brukte, og kor lenge opplysningane blir lagra.

Dei kan i praksis ha mykje å seie for ivaretakinga av personvernet til brukarane.

7.1.5.2 Standardinnstillingar

Det er vanleg at tilbydarar av sosiale medium lèt brukarane sjølve avgjere tilgangen til ein del av opplysningane dei genererer. Ei utfordring er likevel at standardinnstillingane ofte ikkje er sette til det mest personvernvenlege nivået, og at brukarane ikkje i tilstrekkeleg grad er merksame på standardinnstillingane, kva dei inneber, og korleis dei kan endrast. I meldinga blir det peika på ulike døme.

7.1.5.3 Tredjepartars bruk av personopplysningar

Gjennom digitale spor får kommersielle nettenester store mengder opplysningar som dei kan nytte til marknadsføring. I sosiale medium legg brukarane igjen personopplysningar i byte mot tenester. Datatilsynet stilte i juni 2011 ei rekkje spørsmål til Facebook om innsamling og bruk av personopplysningar. Facebook stadfesta i svarbrevet til Datatilsynet at det innhaldet brukarane skriv på sida si, blir brukt til å

målrette reklame. Det er ei viktig oppgåve å hindre at kommersielle nett-tenester registrerer, lagrar og utnyttar digitale personopplysningar på måtar som trugar integriteten og sjølvråderetten til den einskilde.

7.1.5.4 Sletting

I 2011 fekk slettmeg.no (sjå meir om denne tenesta nedanfor) over 6 000 personlege førespurnadar. Det blir i meldinga vist til at det er ei utfordring i dag at mange tilbydarar av sosiale medium anten ikkje aksepterer sletting, eller at dei er så gode til å skjule informasjon om korleis ein kan slette personopplysningar eller melde seg ut av tenesta, at brukarane ikkje finn ut korleis dei skal gjere det.

I tillegg er det ei utfordring at sletting av ein konto ikkje alltid inneber sletting av opplysningar som er kopla til kontoen.

7.1.6 Særleg om Facebook

Det blir i meldinga vist til at Facebook er eit viktig sosialt medium for mange. Ein reknar med at over 2,7 millionar nordmenn har brukarprofil på Facebook (tal frå Ipsos MMI oktober 2012).

Mange av personvernbekymringane som har kome til uttrykk ved ulike revisjonar av Facebook, er òg aktuelle for andre sosiale nettverk. Kombinasjonen av lite informasjon til brukarane og til dels manglande høve for brukarane til å påverke korleis personopplysningane deira blir brukte, gjer at brukarane kan miste kontroll over eigne opplysningar. Dette kan tale for at ein burde stille strengare krav til samtykke til behandling av personopplysningar i sosiale nettverk. Det bør òg stillast strengare krav til utforminga av verktøy som gjer at brukarane kan kontrollere korleis personopplysningane knytte til dei, blir behandla. Ein kan for eksempel tenkje seg å gjennomføre dette ved å utarbeide meir detaljerte norske retningsliner for kva informasjon som bør liggje til grunn for samtykke, og kva tekniske val og funksjonar som skal vere tilgjengelege for brukarane av sosiale nettverk.

7.1.7 Ansvaret til den einskilde og det offentlege

Det er kvar einskild som har ansvaret for å setje seg inn i gjeldande vilkår for den tenesta han eller ho er brukar av, og stå til ansvar for det ein sjølv har publisert. For vaksne kan dette verke nokså sjølvsagt. Likevel gjer kompliserte brukarvilkår det vanskeleg å setje seg inn i korleis personopplysningar blir behandla i mange sosiale medium. Sidan ein stor del av brukarane av sosiale medium er barn og unge, som ikkje har same føresetnadene som vaksne for å setje seg inn i brukarvilkåra, bør tenestetilbydarane ta omsyn til det når dei utformar vilkår og design for tenestene.

Gjennom informasjonsarbeid tek også det offentlege eit ansvar for å førebyggje krenkingar på nett.

7.1.7.1 Trygg bruk

Medietilsynet sitt Trygg bruk-prosjekt fungerer som det nasjonale koordineringsorganet for initiativ retta mot å fremje trygg og sikker bruk av digitale medium for barn og unge.

7.1.7.2 Nettstaden Nettvett.no

Nettvett.no er ein nettstad der brukarane finn informasjon, råd og rettleiing om trygg bruk av Internett. Informasjonen er retta både mot forbrukarar og små og mellomstore bedrifter.

7.1.7.3 Du bestemmer

Undervisningsprogrammet Du bestemmer er eit samarbeidstiltak mellom Teknologirådet, Datatilsynet og Senter for IKT i utdanninga. Målet er å gi barn og unge betre kunnskap om personvern og gjere dei meir medvitne om val dei tek når dei bruker digitale medium som Internett og mobiltelefon.

7.1.7.4 Nødhjelp

På oppdrag frå Fornyings- og administrasjonsdepartementet laga Datatilsynet ei utgreiing om korleis ei slettehjelpsteneste kunne driftast, og leverte forslaget sitt til departementet den 30. januar 2009. Slettmeg.no vart lansert i mars 2010. Føremålet med tenesta er å gi råd og rettleiing om korleis ein kan slette uønskt og personvernkrenkjande materiale som ligg på nett, men i særlege tilfelle kan ho òg yte praktisk bistand til å slette slikt materiale.

Datatilsynet hadde ansvar for drift av slettmeg.no i 2010 og 2011. Ansvaret for slettmeg.no vart frå og med januar 2012 overført frå Datatilsynet til Norsk senter for informasjonssikring (NorSIS). Der blir tenesta no driven vidare på permanent basis.

I 2011 gjaldt den vanlegaste typen førespurnader sletting av eigen profil på nettet.

Uønskt biletpublisering på Internett er eit stort problem i dag. 11 pst. av alle førespurnadene som kom til slettmeg.no i 2011, gjaldt bilete som nokon hadde lagt ut mot klagaren sin vilje.

Det blir allereie gjort mykje godt førebyggjande arbeid. Regjeringa er oppteken av å utnytte ressursane best mogleg for å få gode tenester som er lett tilgjengelege for publikum. Betre samordning av arbeidet kan vere eit alternativ for å nå dette målet. Regjeringa ønskjer derfor å vurdere om det er mogleg å samordne ulike haldningsskapande tiltak for å redusere talet på og omfanget av nettkrenkingar.

7.1.8 Personvern og ytringsfridom på nett

Det blir i meldinga peikt på at personvern og ytringsfridom er godt forankra både i norsk og internasjonal lovgiving. I norsk lovgiving er tilhøvet mellom personvern og ytringsfridom regulert i personopplysningslova § 7, som gjennomfører personverndirektivet artikkel 9. Reglar om ytringsfridom og personvern finst òg fleire andre stader i norsk lovgiving (sjå meldinga).

Ny teknologi gjer det enkelt å publisere informasjon på Internett, og tilgangen på informasjon aukar. Dette aktualiserer spørsmål om korleis personvern og ytringsfridom skal balanserast mot kvarandre.

Det har i lengre tid vore ei utfordring at reglane i personopplysningslova ikkje har omfatta visse ytringar på nett, fordi ytringane har vore framsette med «opinionsdannande» føremål. Slike ytringar har ikkje vore omfatta av reglane i lova, jf. personopplysningslova § 7. Sjå meldinga for nærmare omtale.

Sett i lys av dei mange moglege måtane som finst til å publisere personopplysningar på nett, tyder praksis og vurderingar om personvern og ytringsfridom på at dette er eit område der det òg i framtida vil vere utfordringar.

7.1.9 Råderettsalder på nett

Hovudregelen er at mindreårige som har fylt 15 år, sjølve kan samtykkje i innhenting og bruk av eigne personopplysningar. For barn under 15 år må eventuelt foreldre/føresette samtykkje i innhenting og bruk av opplysningar om barnet. For innhenting og behandling av sensitive personopplysningar, for eksempel helseopplysningar, opplysningar om livssyn og seksuelle forhold, krevst det uansett samtykke frå foreldra fram til barnet er myndig. Både den mindreårige og dei føresette kan når som helst trekkje tilbake eit samtykke. Opplysningane skal slettast når samtykket er trekt tilbake.

Det kan vere gode grunnar til å vere varsam med kva opplysningar som blir publiserte om barn og unge på Internett.

Når barn og unge er målgruppa, må det leggjast til rette for at dei skal forstå konsekvensane av å samtykkje i at personleg informasjon kan leggjast på nettet. Informasjonen som blir gitt, må blant anna vere tilpassa barns kognitive evner. Ivaretaking av barns rettar kan by på særlege utfordringar når personlege opplysningar blir publiserte på internasjonale nettsider der norske reglar om vern av barn ikkje gjeld.

7.1.10 Sletting av opplysningar på nett om avdøde personar

Personvernet gjeld for levande personar. Personopplysningslova vernar opplysningar om avdøde berre dersom opplysningane også seier noko om levande personar, for eksempel opplysningar om gen. Ein kan derfor sjeldan bruke reglane i personopplysningslova for å få uønskte opplysningar om avdøde personar fjerna frå nettet. I 2011 tok slettmeg.no imot 234 førespurnader frå personar som ønskte å få fjerna ein profil eller konto til ein familiemedlem eller ein ven som hadde gått bort.

Det blir i meldinga peikt på at det er legitime grunnar til at personopplysningar om avdøde personar skal ha same vernet som personopplysningar om levande personar. Frå ein norsk ståstad kan det diskuterast om det er praktisk og riktig at personopplysningslova ikkje gjeld avdøde personar.

7.1.11 Hovudpunkt kapittel

- Kommunikasjon i sosiale medium kan innebere ei utfordring for ivaretakinga av personvernet til brukarane.
- Personvernutfordringane i sosiale medium er overnasjonale og gjer det nødvendig med internasjonalt samarbeid.
- Personvernet til barn og unge er særleg utsett på nett. Det må setjast av ressursar til å vidareføre og styrkje førebyggjande arbeid i form av opplysningsverksemd.
- Det bør vurderast ei betre samordning av dei ulike netthjelpstiltaka.

7.2 Komiteens merknader

Komiteen understreker at mange nettsteder kjennetegnes av å være uten kontroll av en redaktør, og uten profesjonelle eller etiske normer å rette seg etter. At flere tilbydere står utenfor norsk rettshåndhevelse, gjør det påkrevet med internasjonalt engasjement for å påvirke regeldannelsen i de internasjonale fora hvor Norge deltar.

Komiteens medlemmer fra Fremskrittspartiet mener sosiale medier er en del av den digitale virkeligheten de fleste befinner seg i. Disse medlemmer viser til at annen teknologi har vært viktig for å nedkjempe diktaturer og totalitære ideologier i vår nære historie. Disse medlemmer viser til at kopieringsmaskiner, telefakser, telex og vanlig trykkpresse var viktige virkemidler for mangfoldiggjøring av informasjon som dissidentgrupper i Sentral- og Øst-Europa formidlet på 1980- og 1990-tallet for å bringe sine diktaturer i kne.

Komiteens medlemmer fra Fremskrittspartiet, Høyre og Kristelig Folkeparti er enig i den gjennomgående problematisering av at barn og unge på grunn av manglende evne til å overskue konsekvensene, kan få sitt personvernvern truet langt utover det tidspunkt man har kommet i skade for å legge ut bilder eller

opplysninger som er av privat karakter. 6 000 henvendelser siden starten til slettetjenesten slettmeg.no sier sitt. Viktige leverandører av nettjenester som Google, Facebook, Twitter o.a. er imidlertid internasjonale, sterke aktører stort sett utenfor norsk jurisdiksjon. Deres sterke stilling overfor unge brukere kan bare balanseres gjennom et målrettet internasjonalt samarbeid, i første rekke gjennom EU.

Disse medlemmer forventer tilbakemelding om hvilke bestrebelser som vil bli gjort, og resultater som oppnås, for å sikre norske barn og unge en sterkere stilling og større råderett over opplysninger om egen person.

8. IKT – utsikter og utfordringar

8.1 Sammendrag

8.1.1 Utviklingstrekk og trendar som verkar inn på sikringa av personvernet

Det blir i meldinga vist til at viktige teknologiske utviklingstrekk som har mykje å seie for samfunnet generelt, er auken i bruk av Internett, sosiale medium, nye lagringsmedium og utsetjing av tenester, for eksempel lagring i nettskya. Fordelane ved dei nye bruksområda er opplagde, medan det kan ta lengre tid å setje seg inn i ulempene og risikoane. Forslaget frå EU-kommisjonen til ei generell forordning om personvern blir grunngitt mellom anna i teknologiutviklinga.

Teknologiutviklinga er prega av innovasjon og rask utvikling med ein påfølgjande vilje i samfunnet til å bruke nye og effektive verktøy. Den raske utviklinga kan seiast å ha både positive og negative konsekvensar for personvernet.

8.1.1.1 Personprofilering og informasjonshandel

Personopplysningar og annan informasjon om forbrukarar har vorte ei av dei største handelsvarene for heile spekteret av IT-verksemder verda rundt. Ikkje berre samlar dei aller fleste Internett-aktørane inn informasjon om sine eigne brukarar, men det har òg vakse fram ein økonomi i det å selje brukarprofilar til tredjepartar, noko stadig fleire aktørar spesialiserer seg på.

Ei utfordring ved det at informasjonshandelen skjer på mange ulike plattformer, er at desse har store tekniske forskjellar, og at tilgangen til gode personverninnstillingar varierer. Det er ikkje enkelt å regulere innhenting av personopplysningar på ein einskapleg måte som tek omsyn til forskjellane mellom plattformene.

8.1.1.2 Nettskya

Dei siste åra har ein sett ein tydeleg auke i utviklinga av ulike tenester baserte på nettskyteknologi, eller Cloud Computing. Både næringsliv og privatpersonar bruker nettskytenester. Somme offentlege verksemder har òg teke i bruk slike tenester til lagring og som programvare. Bruk av nettskytenester inneber at arbeidsoppgåver knytte til IT-funksjonar eller IT-tenester blir sette ut, medan ansvaret framleis ligg hos verksemda som set ut oppgåvene. Nettskyleverandørane er altså å rekne som databehandlarar etter personopplysningslova § 2 nr. 5.

Nettskytenester er ei samlenemning på alt frå databehandling og datalagring til programvare på tenarar som er tilgjengelege frå eksterne tenarparkar knytte til Internett.

Det blir i meldinga peikt på at det ligg eit stort potensial i auka bruk av nettskytenester. Den behandlingsansvarlege sjølv treng ikkje tilsvarande lagringskapasitet og kunnskap om IT-infrastruktur. Dette fører òg til mindre behov for IT-rådgiving og vedlikehald. Bruken av nettskytenester kan òg bidra til å effektivisere datasystem. Nettskya er dessutan fleksibel på den måten at når den behandlingsansvarlege treng meir lagringskapasitet, leiger han det. Dette reduserer dei store kostnadene som følgjer med store IKT-investeringar.

Bruk av nettskytenester reiser samstundes òg visse personvernutfordringar. Mange eksterne tenarparkar ligg utanfor Noregs grenser, og utfordringa for dei behandlingsansvarlege er å sørgje for at avtalene med nettskyleverandøren er i samsvar med norsk lovgiving. Det kan vere krevjande å sikre at ein fyller krav til sikring av informasjon og reglane om overføring av personopplysningar til statar utanfor EU/EØS-området. Databehandlaravtaler skal normalt innehalde punkt om graden av informasjonstryggleik og kva slags tiltak som skal setjast i verk ved eventuelle tryggleiksbrot. I samband med dette må den behandlingsansvarlege gjere grundige risikovurderingar baserte på informasjon frå nettskytilbydaren. Dersom risikovurderingane ikkje er godt nok gjennomførte og dokumenterte, risikerer brukarar av nettskytenester at nettskytilbydaren skriv frå seg ansvaret dersom informasjon kjem på avvegar.

Det blir i meldinga vist til at det kan tenkjast at mange behandlingsansvarlege, særleg små og mellomstore verksemder, vil få betre trygging av personopplysningar når dei bruker nettskytenester. Utfordringa er å finne løysingar på dei informasjonsbarrierane som hindrar tenesteleverandørane i å dokumentere tryggleiksnivået overfor kunden. I meldinga blir det peika på at ei løysing med jamleg revisjon av ein uavhengig tredjepart kan vere ei mogleg løysing på dette problemet.

Kontrollane Datatilsynet gjer av verksemder som bruker nettskytenester, har avdekt manglande oversikt hos verksemdene over kva problem dei må ta stilling til, og korleis dei skal gå fram for å sikre personvernet på best mogleg måte. I meldinga blir det peikt på at det må stillast klåre krav til kva risikovurderingar dei behandlingsansvarlege skal gjere, og kva tryggleiksnivå dei ulike aktørane bør liggje på. Gjennomsiktige prosedyrar er nødvendig for at den behandlingsansvarlege skal kunne forvisse seg om at all aktivitet skjer innanfor rammene av norsk personvernlovgiving. Det er her viktig å samarbeide med nettskyleverandørane for å kome fram til løysingar som begge partar kan seie seg fornøgde med, og som på best mogleg vis sikrar personvernet til dei registrerte. Det er òg viktig at norske behandlingsansvarlege både i offentlege og private verksemder blir sette i stand til å gjere gode og rette vurderingar av risiko og personvern når dei inngår slike avtaler.

EU-kommisjonen er òg oppteken av å møte utfordringane og nytte det potensialet som ligg i nettskya. Kommisjonen kom med ein kommunikasjon i september 2012 der dei skisserer tre hovudmål for nettsky i EU.

Det går fram av meldinga at Noreg vil følgje med på EU si politikkutvikling på dette området. Ein arbeider òg med dette på nordisk nivå, i regi av Nordisk ministerråd sitt sekretariat. Noreg deltek i dette arbeidet. Regjeringa ser at skytenester kan bidra til rimelege og fleksible løysingar, både for næringslivet og offentlege verksemder. Regjeringa ønskjer derfor å leggje til rette for sikker og forutsigbar bruk av slike tenester innanfor rammene av det norske regelverket, blant anna ved å utarbeide rettleiingar.

8.1.1.3 Biometri

Biometrisk teknologi er ei nemning på teknologiar som identifiserer eller stadfestar identiteten til enkeltindivid ved å analysere dei fysiske eigenskapane og åtferda deira. Eksempel på dette kan vere analysar av fingeravtrykk, andletsgeometri, iris, stemme, gangart eller handskrift/tastetrykk.

Bruken av biometrisk teknologi har auka mykje dei siste ti åra, mykje på grunn av den betra tryggleiken som teknologien gir rundt identiteten og autentisiteten til personar.

Biometri kan seiast å vere meir robust enn andre metodar, ettersom dei fysiske eigenskapane og åtferda til ein person til ein viss grad er konstante. Biometri er òg individualiserande, ettersom dei biometriske eigenskapane stort sett berre kan knytast til éin person. Ein kan hevde at biometri òg er meir tilgjengeleg enn andre metodar. Enkelte biometrimetodar er det lettare for folk å godta enn andre. På den andre sida kan enkelte biometrimetodar opplevast som eit særleg stort inngrep i integriteten, for eksempel bruken av åtferdsbasert biometri, til dømes ganglagsbiometri.

I dag blir biometri først og fremst brukt til ulike typar tilgangskontroll. System for passkontroll bruker i aukande grad biometri for å kunne slå fast at det er rett person som viser fram eit bestemt pass. Biometri kan òg brukast til andre typar tilgangskontroll, for eksempel til å gi fysisk tilgang til avgrensa område eller tilgang til å kjøpe varer med aldersgrense i butikk.

Mange biometrimetodar er enno ikkje i bruk i særleg stor grad, men er under utvikling og på god veg til å bli testa for kommersiell bruk. Ein av desse metodane er den såkalla «face in the crowd»-teknologien. Metoden går ut på at ein installerer videokamera på avgrensa område som skal filme dei som til kvar tid oppheld seg der.

Ei anna form for biometri som ein har prøvd å ta i bruk mellom anna i Storbritannia, er ganglagsbiometri. Ved å studere ein video av ein bestemt person, for eksempel frå overvakingskamera, og ta mål av silhuetten og rørslene til vedkomande kan personen bli attkjend frå eitt kamera til eit anna.

Sjølv om det er mange fordelar knytte til bruken av biometri, skaper metoden òg ei viss uro med tanke på personvern og tryggleik. Det er til ein viss grad mogleg å reprodusere eller imitere biometriske data, for eksempel fingeravtrykk. Dette kan føre til forfalsking av biometriske trekk.

Ytre faktorar kan medverke til å redusere kvaliteten på dei biometriske dataa eller samanhengen mellom data og person.

Bruk av biometri fører òg med seg andre personvernrisikoar enn faren for feil i systemet eller registreringsprosessen. Visse typar biometri, for eksempel «face in the crowd»-teknologien, fungerer under den føresetnaden at dei som blir skanna inn for å bli kryss-sjekka mot registeret, ikkje veit om det. Det kan òg tenkjast at visse typar biometriske data kan avsløre sensitiv informasjon, til dømes om helsetilstand.

Bruken av biometri er i dag regulert av personopplysningslova § 12. Bruk av «entydige identifikasjonsmidler» er berre tillate dersom det er sakleg behov for sikker identifisering, og dersom metoden er nødvendig for å oppnå slik identifisering. Det blir i praksis stilt strenge krav til kriteriet om at bruken er nødvendig, og dersom andre metodar kan brukast til å oppnå det same, er det ikkje tillate å bruke biometri.

I stadig fleire av dei biometriske systema som blir nytta i dag, er det lagra malar av biometriske eigenskapar framfor detaljerte avtrykk, for eksempel fingeravtrykksmalar eller andletsmalar baserte på punkt. Personvernnemnda har i fleire vedtak konkludert med at malar av fingeravtrykk ikkje kan definerast som personopplysningar med mindre dei blir

knytte til annan identifiserande informasjon, som namn, fødselsnummer eller andre personopplysningar. Malane kan ifølgje nemnda ikkje i seg sjølve reknast som «entydige identifikasjonsmidler». Det ser ut til at skiljelinene mellom identifisering og autentisering, som bruken av biometriske malar ofte inneber, må avklårast nærmare.

Det har vore ein gradvis auke i bruken av biometri både hos offentlege og private aktørar og både til autentisering og identifisering. Regjeringa ser at det er klåre fordelar ved utvida bruk av biometri på nye område og er positiv til utviklinga av denne typen teknologi. Det er likevel nødvendig å ha ei bevisst haldning til kva føremål som skal kunne gi grunnlag for å ta i bruk biometri. Det er uheldig å bruke biometri til å identifisere eller autentisere enkeltpersonar i situasjonar der det ikkje er absolutt nødvendig. Bruken av biometriteknologi til reint kommersielle føremål er problematisk dersom det ikkje blir stilt strenge krav til frivillig medverknad og samtykke frå dei registrerte.

8.1.2 Verkemiddel for å oppnå eit best mogleg personvern

Den teknologiske innovasjonstakta står ofte i motsetning til dei tidkrevjande demokratiske reguleringsprosessane. Det er derfor viktig å vurdere andre og meir dynamiske verkemiddel som kan sikre samspelet mellom personvern og teknologisk innovasjon i tillegg til tradisjonell regulering. Bruk av IKT kan utfordre personvernet. Samstundes kan riktig bruk av IKT gi godt grunnlag for å ta vare på personvernet. Nedanfor blir det gjort greie for enkelte forslag til metodar og verkemiddel som kan nyttast for å sikre personvernet når IKT blir teke i bruk.

8.1.2.1 Teknologinøytral lovgiving

Det blir i meldinga peikt på at for å sikre at det kontinuerleg blir utvikla ny og innovativ teknologi, er det viktig at ein ikkje har for store lovhinder for arbeidet til forskarar og utviklarar. Lovgiving som stiller strengare krav til visse typar teknologiar enn til andre, kan vere eit slikt hinder.

Målet om ei teknologinøytral lovgiving følgjer ikkje direkte av lovgivinga, men kan utleiast av Grunnlova § 100 sjette leddet, som pålegg styremaktene å leggje forholda til rette for ei open og opplyst offentleg samtale. Denne føresegna blir gjerne omtala som infrastrukturkravet.

8.1.2.2 Innebygd personvern

Tanken om innebygd personvern («privacy by design») inneber at omsynet til personvernet skal vere ein del av alle ledd i utviklinga og bruken av informasjonsteknologi.

Internasjonalt har innebygd personvern vore eit mål i ei årrekkje. Norske aktørar har fram til no i liten grad engasjert seg i dei prinsippa og det vinstpotensialet som ei slik proaktiv sikring av personvernet kan gi.

Situasjonar der innebygd personvern med fordel kan takast i bruk, er når ein skal utvikle nye register.

I meldinga blir ordninga med e-resept nytta som eit eksempel på innebygd personvern (sjå nærmare omtale).

Innebygd personvern som mål

Prinsippet om innebygd personvern er samansett. Oppdragsgivarar må innarbeide personvern som ein grunnleggjande verdi i verksemda, og utviklarar må vere bevisste på å gjere spørsmål om personvern til ein integrert del av utviklinga og utforminga av produkta og systema sine. I tanken om innebygd personvern ligg det òg at ein skal ta utgangspunkt i å bevare eit best mogleg personvern når ein skal halde ved like og oppdatere IKT-system og informasjonsteknologi. Dei automatiske førehandsinnstillingane i IKT-system og informasjonsteknologi bør ta utgangspunkt i den mest personvernvenlege løysinga, slik at brukaren sjølv kan avgjere om han eller ho ønskjer å ta i bruk ei mindre personvernvenleg løysing der det er mogleg.

Det blir i meldinga peikt på at bruk av teknologi bør skje på ein måte som fremjar personvernet. Kunnskap og medvit er ein spesielt viktig del av prosessen med å byggje personvernet inn i alle dei systema innbyggjarane møter i kvardagen. Ein del av prosessen med å oppnå innebygd personvern handlar om informasjon og om at informasjonen må vere klår. Informasjonskampanjar er berre éin måte å opplyse brukarane om problemstillingar knytte til personvern på. Ein annan og kanskje viktigare måte er å nytte informasjonen brukarane får når dei nyttar IKT-system, nemleg den som finst i personvernpolicyar, såkalla «Terms of Service»- og «Terms of Use»-avtaler, og elles på nettsidene til ulike aktørar. Det blir i meldinga peikt på at brukarvenlege opplegg må vere eit mål for alle aktørar, og at samarbeid om brukarvenlege standardar kan vere ein måte å sikre at folket får meir kunnskap om personvern på.

Ei innvending mot innebygd personvern kan vere at for sterkt personvernfokus blant teknologar og utviklarar kan verke hemmande på innovasjon og teknologisk nyskaping. Det kan dermed òg gå ut over konkurransedugleiken til teknologien. Det blir i meldinga peikt på at eit langsiktig mål må vere å utvikle standardar og bransjenormer som skal gjelde for teknologiutviklarar uavhengig av kor store aktørane er, og på tvers av landegrensene. Dette krev internasjonalt samarbeid. Det er god grunn til å tru at det er lettare for aktørane å etterleve personvernkrav som

blir stilte gjennom bransjenormer og standardar. Sertifiseringsordningar, der styremaktene ope går god for at ein aktør praktiserer ein tilfredsstillande grad av personvern i aktivitetane sine, kan òg gi desse aktørane insentiv til i større grad å byggje personvern inn i heile praksisen.

8.1.2.3 Personvernfremjande teknologi

Personvernfremjande teknologiar («privacy-enhancing technologies» eller PETs) er tekniske løysingar og teknologiar som er utvikla med det konkrete føremålet å verne om personopplysningane til brukarane. Anonymiseringsverktøy og verktøy for å slette historikk i nettlesarar er eksempel på personvernfremjande teknologiar. PETs skil seg frå innebygd personvern på den måten at dei blir implementerte i teknologiar, system og praksisar som allereie eksisterer.

Tradisjonelt har ein sett på PETs som tekniske og organisatoriske tiltak for å kontrollere moglege måtar å identifisere brukaren på. Eit eksempel på bruk av personvernfremjande teknologi i offentlege verksemder er implementeringa av ein immuniseringsfunksjon for søkjemotoren i Offentleg elektronisk postjournal (OEP).

Ein annan og særleg aktuell type personvernfremjande teknologi er «do not track»-teknologien. «Do not track» er ein nettstandard som gjer at brukaren kan gi uttrykk for at han eller ho ikkje ønskjer at nettsidene han eller ho besøkjer, skal sporast på tvers av nettstader. Standarden blir brukt i nettlesarar og inneber at det blir lagt til ein beskjed i adressefeltet i nettlesaren – «do not track» – som fortel nettsida at brukaren ikkje ønskjer å bli spora av tredjepartar. World Wide Web Consortium (W3C) har oppretta ei «do not track»-arbeidsgruppe for å få standardisert denne teknologien. Fleire av dei største Internett-aktørane i verda er representerte i gruppa. Ho arbeider med ein felles standard for «do not track» som alle aktørar som sporar brukarar på nett, bør nytte. Arbeidet til gruppa har fått positiv respons frå EU-hald. Dersom den endelege tilrådinga frå gruppa er tilfredsstillande, vil regjeringa leggje til rette for at «do not track»-standarden blir implementert og etterlevd på nettstadene til norske offentlege og private verksemder.

8.1.2.4 Bruk av standardar/bransjenormer

Det kan vere lite føremålstenleg at styremaktene detaljstyrer praktiseringa av personverntiltak på område der det finst bransjeorganisasjonar som er betre rusta til å vurdere kva behov og problemstillingar som særmerkjer bransjen. Utarbeiding av personvernvenlege standardar og bransjenormer kan vere ein raskare og meir effektiv måte å implementere personvern på enn at styremaktene regulerer det. I meldinga blir bransjenorm for personvern og informasjonstryggleik i elektronisk billettering og norm for informasjonstryggleik i helse- og omsorgssektoren gjort nærmare greie for.

8.1.3 Informasjonstryggleik og personvern

Det blir i meldinga peikt på at informasjonstryggleik er eit viktig verkemiddel for å sikre godt personvern.

Eit overordna bilete av dagens situasjon når det gjeld informasjonstryggleik i Noreg, er gitt i stortingsmeldinga om samfunnstryggleik.

For å møte tryggleiksutfordringane på IKT-området har regjeringa laga ein nasjonal strategi for informasjonstryggleik.

Regjeringa har i budsjettproposisjonen for 2013 føreslått å løyve ekstra midlar til Direktoratet for forvaltning og IKT (Difi) slik at direktoratet kan etablere eit kompetansemiljø som skal arbeide med å betre informasjonstryggleiken i statsforvaltninga.

Sjølv om styremaktene har eit overordna ansvar for å sikre informasjonstryggleik i sektorane sine, har lovgivaren føresett at den behandlingsansvarlege set i verk tilstrekkelege tiltak for å hindre at data kjem på avvegar. Verksemdene må gjere ei risikovurdering ut frå sin eigen situasjon.

8.1.3.1 Konfidensialitet, integritet og tilgang

Informasjonstryggleik etter personopplysningslova § 13 handlar om å verne personopplysningar tilstrekkeleg med omsyn til fortrulegskap, integritet og tilgang. Dette inneber i praksis å sikre desse tre likeverdige føremåla:

– vern mot uautorisert innsyn i personopplysningane (konfidensialitet)
– vern mot uautorisert endring av personopplysningane (integritet)
– tilgang til relevant informasjon til rett tid

Det må setjast i verk tiltak for å oppnå dette.

Mangel på god informasjonstryggleik i ei verksemd kan føre til at tilliten hos den registrerte og samarbeidande verksemder blir redusert.

8.1.3.2 Verkemiddel for å oppnå informasjonstryggleik

Kontrolltiltak

Kontrolltiltak som kan takast i bruk for å styrkje informasjonstryggleiken, er for eksempel å vedta lover og forskrifter eller utarbeide bransjeavtaler og -normer. I dag har ein fleire eksempel på slike reglar, mellom anna i personopplysningslova, ekomlova,

esignaturlova, eforvaltnings- og IKT-forskriftene og tryggingslova.

Ei anna form for kontrolltiltak er dei av økonomisk art. Insentivordningar, skattelettar eller at verksemdene ikkje blir bøtelagde, er alle eksempel på slike økonomiske verkemiddel.

Dei organisatoriske tiltaka er òg ein viktig type kontrolltiltak. Verksemder bør med jamne mellomrom risikovurdere eigne informasjonssystem og ordningar for å avdekkje sårbare punkt og eventuelt setje i gang sikringstiltak. Ein annan måte å sikre informasjon gjennom organisatoriske tiltak på, er å styre tilgangen til informasjon eller gradere informasjon og kommunikasjonsnivå.

Informasjonstiltak og haldningsskapande arbeid

Informasjonstiltak er òg eit viktig verkemiddel for å oppnå god informasjonstryggleik. Datatilsynet, Nasjonalt tryggingsorgan, NorSIS og Difi gjer alle eit viktig arbeid med å utarbeide rettleiingar og informasjonsskriv til verksemder som treng hjelp til å praktisere god informasjonstryggleik. Regjeringa er svært positiv til informasjonsarbeidet desse aktørane utfører, og meiner dette arbeidet bør halde fram.

I tillegg til at verksemder som behandlar personopplysningar har tilgang til generell informasjon om informasjonstryggleik, er det viktig at både verksemder og enkeltpersonar faktisk set pris på god informasjonstryggleik. Det er derfor viktig at det blir drive godt haldningsskapande arbeid, og at ein skaper ein god kultur for informasjonstryggleik hos norske aktørar.

Teknologiske tiltak

Det blir i meldinga peikt på at det er dei teknologiske sikringstiltaka som er absolutt viktigast i arbeidet med å oppnå informasjonstryggleik.

Det er lettare å oppretthalde god informasjonstryggleik i dei enkle informasjonssystema enn i dei kompliserte. Ein måte å løyse dette problemet på er å dele systemet inn i nokre få pålitelege komponentar og fleire potensielt upålitelege komponentar. Mesteparten av informasjonen blir lagra i dei mindre pålitelege komponentane, medan den viktigaste og mest sensitive informasjonen blir lagra i dei pålitelege komponentane. Denne organiseringa går under namnet Trusted Computing Base (TCB).

Vidare er det viktig for å halde ved lag god informasjonstryggleik at det blir brukt programvare som sikrar at uvedkomande ikkje får tilgang til systemet.

Løysingar for avbrotsfri straumforsyning kan bidra til å sikre tilgangen til eit system. Ei anna løysing som kan sikre tilgangen til eit system, er bruk av alternative nettverk.

Kryptering av viktig informasjon og kommunikasjon er ein tryggleiksføresetnad for større, meir kompliserte og dermed òg meir sårbare informasjonssystem. Dei to alternative metodane for kryptering er kanalkryptering og innhaldskryptering, sjå nærmare omtale i meldinga.

System for identitetsforvalting, tilgangskontroll og logging er blant dei viktigaste teknologiske verkemidla for informasjonstryggleik. Problemstillingar som gjeld identitetsforvalting, tilgangskontroll og logging blir nærmare omtala i meldingas kapittel 9.5.

8.1.3.3 UTFORDRINGAR

Det blir i meldinga peikt på at den største personvernutfordringa når det gjeld tryggleik, knyter seg til det å verkeleg få sett informasjonstryggleik på agendaen i norske verksemder. Først når verksemdene har teke regelverket inn over seg, bestemt seg for å etterleve det, gjennomført nødvendige prosessar og arbeidd med å gjere tryggleik til ein del av kulturen i verksemda, har dei oppnådd intensjonen med regelverket. Det er viktig å ha ei balansert tilnærming til kombinasjonen av verkemiddel.

Det blir i meldinga peikt på at det òg er viktig at ein med jamne mellomrom drøftar behovet for nye sikringsmetodar for IKT-systema i både offentlege og private verksemder.

Arbeidet styremaktene gjer, bør òg i framtida vere ein kombinasjonen av tilsyn, rettleiing og informasjon. Ein bør intensivere arbeidet med å få til ei betre koordinering av regelverket. I dette arbeidet bør departementa ha ei sentral rolle.

8.1.4 Elektroniske spor

Nordmenn lever i aukande grad i ein teknologisk og interaktiv kvardag. Heile dagen igjennom lèt innbyggjarane etter seg ein stig av elektroniske spor.

Desse spora kan følgjast av ulike aktørar, for eksempel politiet, finansinstitusjonar og sosiale nettverk.

Samfunnet blir meir og meir avhengig av å ha velfungerande elektroniske kommunikasjonsnett og -tenester. Bruk av elektronisk kommunikasjon lèt etter seg detaljerte spor mellom anna om kvar ein oppheld seg, korleis ein bevegar seg, kva omgangskrins ein har, og kva interesser og meiningar ein har. Jamvel når utstyr som mobiltelefonar og nettbrett ikkje er i bruk, men berre aktiverte, kan dei late etter seg elektroniske spor i nettverket dei er kopla opp mot.

Elektroniske spor blir i stadig større grad knytte saman med kvarandre av teknologar, forretningsfolk, offentlege styremakter og analytikarar. Somme hevdar at vi lever i tidsalderen for «Big Data». Eit viktig spørsmål alle bør stille seg, er kva opplysningar som blir innsamla, av kven og til kva føremål.

8.1.4.1 Geolokalisering

Lokaliseringsteknologi er eit tema som har vore mykje diskutert dei siste åra. Datatilsynet har i stadig større grad vorte kontakta om ulike former for lokaliseringsteknologi, særleg GPS-sporing. Denne typen sporing har etter kvart vorte vanleg i store delar av transportsektoren.

Det er i hovudsaka tre typar aktørar som registrerer lokaliseringsdata: ekomtilbydarar, internettleverandørar og enkelte andre Internett-aktørar.

Det blir i meldinga peikt på at ei personvernutfordring når det gjeld bruk av geolokalisering, er at smarttelefonar, og i mange tilfelle datamaskiner, ofte er direkte knytte til enkeltpersonar, og at informasjon om kvar det tekniske utstyret er plassert, derfor ofte er synonymt med informasjon om kvar ein enkeltperson oppheld seg. Sporingsinformasjon om rørslemønsteret til enkeltpersonar er noko ein bør vere svært forsiktig med å bruke. Retten til fri ferdsel og privatliv er grunnleggjande og ukrenkjeleg. Dersom ein skal gjere inngrep i denne retten, må ein ha ein klår lovheimel eller samtykke frå den som blir lokalisert. Når det gjeld mobiltelefonar, er det samtykke som er det aktuelle grunnlaget for bruk av GPS-lokalisering. Det er derfor ei utfordring at mange smarttelefonar i dag har GPS-lokalisering aktivert som førehandsdefinert innstilling.

Eit anna viktig tema er geolokalisering av barn. Teknologien gjer det mogleg for foreldre å GPS-spore sine eigne barn gjennom smarttelefonane deira. Det kan diskuterast om ein slik kontroll inneber ei krenking av barna sitt privatliv og rett til fri ferdsel. Regjeringa helser denne debatten velkomen.

Mange lokaliseringstenester som er i bruk i dag, er aktiverte i dei førehandsdefinerte innstillingane på smarttelefonar og anna utstyr. Lokaliseringsinformasjon er personopplysningar når dei kan knytast til ein kunde eller eit abonnement. Aktivering av lokaliseringstenester krev derfor frivillig, informert og uttrykkeleg samtykke frå brukaren etter norsk lov. Artikkel 29-arbeidsgruppa framhevar i den tidlegare nemnde fråsegna om geolokalisering av smarttelefonar at lokaliseringstenester må vere avslått i dei førehandsdefinerte innstillingane på telefonen for at samtykkekravet skal vere oppfylt. Dei gir òg uttrykk for at samtykke til geolokalisering ikkje kan innhentast gjennom standardvilkår.

8.1.4.2 Sporing av reisande

Ei anna og meir generell form for sporing som òg er omdiskutert, er sporing av trafikantar. Retten til anonym ferdsel har spesielt vore diskutert i samband med kollektivtransport og bompengestasjonar.

Det er innført ei bransjenorm for personvern og informasjonstryggleik innan elektronisk billettering ved årsskiftet 2011/2012. På same måten som ein kan reise anonymt med kollektivtransport ved hjelp av papirbasert enkeltbillett, fleirreise- og/eller periodekort, vil ein ha det same høvet til å reise anonymt med båt, buss, bane og tog ved hjelp av elektronisk billett så lenge bransjenorma for personvern ligg til grunn.

Dei siste åra har òg norske bompengeanlegg i stadig større grad vorte heilautomatiserte via AutoPASS. Desse heilautomatiserte anlegga er effektive og kostnadssparande, men ein kan ikkje passere anonymt ved å betale med mynt.

I samsvar med vedtak i Personvernnemnda blir passeringsdata lagra i ti år. Det finst per i dag eit såkalla «sporfritt alternativ», der passeringsdata maksimalt blir lagra i 72 timar. Når ein vel dette alternativet, seier ein derimot frå seg klageretten, ettersom det ikkje vil gå fram av fakturaen kva bompengeanlegg ein har passert. Datatilsynet er ikkje fornøgd med denne løysinga.

På bakgrunn av dette har regjeringa i stortingsproposisjonen om Oslopakke 3 varsla eit interdepartementalt samarbeid om anonymitet ved passering av bomstasjonar, jf. St.prp. nr. 40 (2007–2008) og oppfølgjande omtale i St.meld. nr. 16 (2008–2009) Nasjonal transportplan 2010–2019.

8.1.4.3 RFID (Radio Frequency Identification) og NFC (Near Field Communication)

RFID (Radio Frequency Identification) er ein metode for å verifisere identiteten til ein ting basert på informasjon som serienummer eller liknande som er lagra i såkalla RFID-brikker.

Ein metode for sporing som baserer seg på RFID, er NFC (Near Field Communication). Ved hjelp av NFC byggjer ein sporingsbrikker inn i ting for å kunne kommunisere med andre ting, med ein maksimal avstand på rundt 10 cm. Kommunikasjonen blir aktivert av ein avlesar som startar kommunikasjonen med brikka. Mobiltelefonprodusentar, ekomtilbydarar og bankar bruker i dag NFC til å gjennomføre ulike typar transaksjonar ved hjelp av brikker som er bygde inn i smarttelefonar og andre berbare apparat. Eit eksempel på system der ein har hatt suksess med bruk av NFC-teknologi, er trikke- og metrosystem.

Denne teknologien er i rask utvikling og kjem til å bli teken i bruk i stadig større grad dei neste åra. Det er god grunn til å tru at teknologien kan erstatte kort- og kontantbetaling for visse typar betaling ved mindre beløp. Nokon nasjonal standard for bruk av NFC-teknologi innan kollektivtransporten i Noreg er førebels ikkje utarbeidd, men det er planlagt å knyte ein slik standard til nasjonal standard for elektronisk billettering.

Eit område som er spesielt aktuelt til bruk av NFC-teknologi i framtida, er marknadsføring. Det er mogleg å overføre informasjon frå avlesarar til brik-

kene, som så kan visast på smarttelefonen. Dette kan utgjere ein heilt ny marknad for åtferdsretta reklame. Ein kjem òg til å kunne lagre biometrisk informasjon i brikkene, noko som for eksempel kan tenkjast å bli brukt i tryggleikskontrollen på flyplassar.

Ei tryggleiksutfordring ved bruken av NFC-teknologi er at det ikkje er noko krav om kryptering av kommunikasjonen mellom smarttelefonane (eller andre ting med sporingsbrikker) og avlesaren. Dette gjer at kommunikasjonen blir sårbar for angrep, for eksempel avlytting, modifisering av data og svindel.

8.1.4.4 Lagring av informasjonskapslar

Det blir i meldinga vist til at informasjonskapslar, eller http-cookies, er den aller vanlegaste sporingsteknologien i bruk på Internett. Det finst svært mange ulike typar informasjonskapslar, og dei blir brukte til mange ulike føremål. Teknisk sett er informasjonskapslar korte tekststrenger som blir sende frå ei nettside til harddisken til brukaren. Desse tekststrengene blir så lagra på harddisken og sende tilbake til nettsida kvar gong brukaren besøkjer denne nettsida att.

Eit spørsmål som ofte kjem opp når ein drøftar informasjonskapslar i eit personvernperspektiv, er om kapslane inneheld personopplysningar. Når utstyret er knytt opp mot Internett, kan kapslane òg knytast opp mot IP-adressa som blir brukt i påloggingsøkta. Sjølv om desse unike identifikatorane og IP-adressene ikkje alltid kan knytast til enkeltpersonar, er det vanskeleg på førehand å seie om tilknytinga er der eller ikkje. I norsk rett ser ein derfor i praksis på lagring av IP-adresser som behandling av personopplysningar. Det blir i meldinga vist til at dette talar for at ein òg bør sjå lagring av informasjonskapslar som behandling av personopplysningar.

Bruken av informasjonskapslar er svært omfattande. Ein stor del av informasjonskapslane som blir lagra av nettsider i dag, er det gode grunnar til å lagre. Mellom anna er informasjonskapslar nødvendige for at ein skal kunne aktivere automatisk innlogging på nettsider og for å hugse informasjon om handelstransaksjonar frå ei nettsidevising til ei anna. Likevel er det viktig å skilje mellom lagring av informasjonskapslar for å gjere nettsider meir brukarvenlege og lagring til reint kommersielle føremål. Desse siste krev at brukaren blir informert om lagringa på førehand. Dette er regulert i ekomforskrifta § 7-3.

Ein stor del av informasjonskapslane som blir lagra på utstyret til brukarane, blir lagra til kommersielle føremål, for eksempel brukarprofilering til annonsesal og reklame.

Ettersom ein har vorte meir bevisste på lagring av kapslane, er det utvikla nye og spesielt hardføre typar informasjonskapslar, mellom anna såkalla «flash cookies», «supercookies» og «evercookies». Det blir i meldinga peikt på at desse typane informasjonskapslar utgjer eit stort trugsmål mot personvernet til brukarane, ettersom brukaren korkje blir informert om eller merkar noko til at dei blir lagra. Det er dermed umogleg for brukaren å late vere å samtykkje eller å slette kapslane når dei først er lagra.

Etter praksis i dag blir informasjonskapslar lagra med heimel i personopplysningslova § 8 a eller f. Lagringa blir då rekna som nødvendig for å kunne oppfylle ei avtale med den registrerte, eller den behandlingsansvarlege blir rekna for å ha ei rettkomen interesse av å lagre informasjonskapslar som ikkje overstig interessa den registrerte har av å sikre sitt eige personvern. På mange av dei vanlegaste nettlesarane er praksisen slik at informasjonskapslar blir lagra på utstyret til brukarane basert på at førehandsinnstillingane i nettlesaren er sette til å godta slik lagring. Brukarar som ikkje ønskjer at informasjonskapslar skal bli lagra, må aktivt reservere seg mot dette ved å endre innstillingane i nettlesaren. Ein praktiserer altså lagring med heimel i nødvendiggjerande grunn, men med ein reservasjonsrett for brukarane.

Krava til lagring av informasjonskapslar er innskjerpa på EU-nivå gjennom kommunikasjonsverndirektivet og tillegget frå 2009, populært kalla «cookie-direktivet». Dette direktivet er EØS-relevant, og regjeringa vil kome tilbake til Stortinget med forslag til gjennomføring av det i norsk rett. Etter artikkel 5 (3) i direktivet blir det no stilt strengare krav til at brukarane sjølve skal samtykkje til lagring av informasjonskapslar som ikkje er heimla i lov, eller blir lagra av tekniske årsaker.

Blant føremåla som etter Artikkel 29-arbeidsgruppa si meining ikkje krev samtykke, er autentisering ved innloggingstenester, memorisering av inntasting i elektroniske skjema eller handlekorger i løpet av ei økt, eller det å gjere det teknisk mogleg å spele av video eller lyd når brukaren ber om det. Føremål som etter arbeidsgruppa si meining derimot krev samtykke, er mellom anna åtferdsretta eller interaktiv marknadsføring og sporing av brukarar gjennom sosiale «plugin-modular», for eksempel Likar-knappen på Facebook.

Spørsmålet om samtykke til lagring av informasjonskapslar har vore mykje omdiskutert. Særleg gjeld dette spørsmålet om ein skal innføre krav om aktivt samtykke, eller om ein skal nøye seg med at brukaren har høve til å reservere seg mot lagring av informasjonskapslar gjennom innstillingar i nettlesaren sin.

8.1.5 Identitetsforvalting: identifisering, autentisering og tilgangsstyring

I IKT-system der store mengder personopplysningar blir behandla, er det eit spesielt stort behov for å ha gode tryggings- og personverntiltak.

Identitetsforvalting vil seie å administrere identitetar, og handlar i vid forstand om å identifisere individ og kontrollere tilgangen til ulike ressursar. Identitetsforvalting femner om registrering, identifisering, autentisering og autorisering.

Medan identifisering dreiar seg om å skilje personar frå kvarandre, handlar autentisering om å slå fast om ein person er den han eller ho gir seg ut for å vere. Ein skil ofte mellom tre måtar å identifisere seg på: gjennom noko ein veit (passord, pin-kodar), noko ein har (smartkort, identitetskort) eller noko ein er (biometri).

Autoriseringa av ein person regulerer kva denne personen kan gjere etter at autentiseringa er gjennomført, for eksempel kva informasjon vedkomande får tilgang til, eller kva oppgåver vedkomande kan utføre.

8.1.5.1 Tillitsnivå

Det finst ulike metodar for å identifisere eller autentisere seg for å få tilgang til eit IKT-system som er identitetsforvalta.

Ein enkel metode er ein-faktor-autentisering, det vil seie at ein autentiserer seg ved bruk av eitt passord. Dette er ein metode som har liten grad av tryggleik. Metoden kan òg kombinerast med å be om eingongspassord, som for eksempel blir sendt til mobiltelefonen til brukaren. Då får ein det som kallast to-faktor-autentisering, noko som har større grad av tryggleik.

Ein annan metode er å bruke innlogging basert på PKI (Public Key Infrastructure). PKI er eit system for å ferde ut digitale sertifikat som stadfestar identiteten til brukaren og at identiteten er gitt av ei offentleg styremakt. PKI er basert på to «nøkkelsett», ein offentleg nøkkel som er tilgjengeleg for alle og blir brukt til å kryptere innhald, og ein privat nøkkel som blir brukt av ein person til å dekryptere innhaldet som vart kryptert med den tilhøyrande offentlege nøkkelen. Ein aktør som leverer løysingar. PKI-teknologien og bruk av nøkkelsett blir rekna for å vere den sikraste teknologien for autentisering av brukarar.

Ein aktuell metode både for identifikasjon og autentisering er å bruke biometri, for eksempel fingeravtrykk- eller irisavlesing. Biometri gir høg grad av tryggleik i den forstand at biometriske trekk i utgangspunktet er uløyseleg knytte til ein person, og at desse trekka normalt ikkje kan overdragast til andre.

Personvernnemda har i løpet av 2012 kome med to avgjerder som opnar for utvida bruk av biometri der ein berre autentiserer og ikkje identifiserer.

8.1.5.2 Tilgangsstyring

Ein har alle ulike roller i ulike situasjonar og til ulike tidspunkt. Desse rollene utviklar og endrar seg med tida, og ein får nye roller samtidig som andre fell bort. Det er òg mange roller som er svært samansette i dei ulike IKT-systema.

Det blir i meldinga vist til at det er krevjande å lage dekkjande roller for tilgangsstyring i IKT-system.

Det er for eksempel viktig å oppdatere tilgangsforvaltinga når nokon sluttar i jobben, eller når nokon begynner å arbeide med nye oppgåver. Det ligg òg ei utfordring i det å utvikle nye roller og nye handlingar i eit system. Kompleksiteten i eit system for identitetsforvalting viser nettopp kor komplekse alle dei ulike rollene våre og tilhøvet mellom dei er.

Det blir i meldinga peikt på at det er viktig at aktørar som bruker system for identitetsforvalting, nyttar metodar for tilgangsstyring som er sikre og effektive. Dersom ein skal oppnå tilfredsstillande og tilpassa tryggleik, bør det leggjast til rette for å bruke løysingar for sikker e-ID framfor passordløysingar og liknande for å få tilgang til register som behandlar sensitive personopplysningar.

8.1.5.3 Løysingar i offentleg sektor

Det som ligg til grunn for autentisering og identifikasjon av innbyggjarar og verksemder mot offentlege digitale løysingar, er Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. Rammeverket består av tilrådingar om korleis ein gjennomfører risikoanalysar og vel tryggleiksnivå når ein skal autentisere brukarar av digitale tenester frå forvaltninga og brukarar i offentleg sektor som kommuniserer internt. Vidare inneheld rammeverket overordna tilrådingar om korleis ein vel tryggleiksnivå når ein har behov for å knyte ein brukar til ein elektronisk transaksjon.

Offentlege verksemder må gjennomføre risiko- og sårbarheitsanalysar når dei etablerer nye elektroniske tenester, og når dei reviderer eksisterande tenester.

ID-porten er ei felles påloggingsløysing for offentlege tenester på nettet. Per desember 2012 kan ein bruke fire ulike elektroniske ID-ar når ein skal logge seg på offentlege tenester. MinID er utvikla og blir drifta av Direktoratet for forvaltning og IKT og plasserer seg på tryggleiksnivå 3, medan elektronisk ID frå høvesvis Bank ID, Buypass og Commfides er plassert på tryggleiksnivå 4.

ID-porten stør berre bruk av identitetsbevis for fysiske personar. Påloggingsløysinga kan nyttast både til å utføre oppgåver i eigenskap av privatperson og til oppgåver på vegner av andre. Det er òg mogleg å opprette identitetsbevis for juridiske personar (for eksempel verksemdssertifikat).

I utdanningssektoren er det etablert ei særleg løysing for tilgangsstyring, Feide (Felles Elektronisk IDEntitet). I Feide-systemet kan skulen sjølv styre kven som skal få tildelt brukarnamn og passord, og kva type brukarkonto dei skal få tildelt. Foreldre vil ikkje sjølve vere Feide-brukarar med eigne brukarnamn og passord. Skulen kan gi dei tilgang ved at deira eiga eID-løysing, for eksempel MinID, blir kopla til Feide-identiteten til barnet deira.

8.1.5.4 Løysingar i privat sektor

Det finst mange ulike autentiseringsløysingar i privat sektor. Bankane har utvikla BankID for pålogging til nettbank, og Norsk Tipping nyttar løysingane frå Buypass for tipping på nett. Saman med tenestene frå den tredje norske aktøren, Commfides, er dette løysingar på tryggingsnivå 4. Alle desse aktørane er sjølvdeklarerte hos Post- og teletilsynet.

I tillegg ser ein tendensar til at også store private aktørar som Facebook og Google innfører eigne system for identitetsforvalting gjennom å tilby påloggingsløysingar for ulike system gjennom Facebook. Origo, som er eit av dei største sosiale nettverka i Noreg, tilbyr for eksempel innlogging gjennom både Facebook, Twitter og Google.

8.1.5.5 Sterkare grep om identitetsforvalting

Grunnidentifisering og registrering av norske borgarars identitet i offentlege register er eit ansvar for styremaktene. Dette skjer i dag ved utferding av fødselsattest og seinare første gongen ein får utferda pass. Utanom pass finst det i dag ingen andre identitetskort utferda av offentlege styremakter.

Dette er noko av bakgrunnen for at regjeringa no arbeider med ei løysing for nasjonalt ID-kort med e-ID i Noreg. Den elektroniske ID-en på kortet vil tilfredsstille krava til nivå 4, og ein vil kunne bruke det til alle offentlege tenester på nett. Ei satsing på nasjonalt ID-kort vil innebere auka tryggleik med tanke på identifisering i det daglege og vil òg heve kvaliteten på utferdinga av andre legitimasjonsbevis i samfunnet. Sikker identifisering er òg viktig for å kunne realisere det målet regjeringa har om eit digitalt førsteval. Tilrettelegging for sikker identifikasjon av norske innbyggjarar er ei viktig oppgåve for styremaktene og står sentralt i innsatsen mot kriminalitet reint allment, mot ID-tjuveri og mot internettkriminalitet.

8.1.6 Innsynslogging

Dersom ein fører kontroll med kva dokument og område kvar enkelt rolleinnehavar bruker eller prøver å bruke, kor lenge og når, kan ein avdekkje og førebyggje ureglementert innsyn. Innsynslogging kan vere føremålstenleg å gjennomføre i store register.

Regjeringa meiner at plikta til å logge og retten til å få innsyn i eigne loggar skal vere eit berande prinsipp for alle større offentlege og private register.

Innsynslogging kan sjåast som ei form for internkontroll og blir i større eller mindre grad brukt i nokre av dei store registera, som helseregistera, politiregistera og Nav-registera. For desse registera må ein opprette klåre loggingskategoriar. Nokre av kategoriane bør derimot vere meir elastiske enn andre.

Verksemdene som er ansvarlege for tilgangsstyringa, må tenkje nøye gjennom kva rammer det skal setjast for tilgangen, og korleis dei vil balansere tilgangen til opplysningar mot omsynet til personvernet basert på ei konkret risikovurdering.

Systema for identitetsforvalting og tilgangsstyring og systema for logging heng slik sett nært saman, og det er ikkje føremålstenleg å praktisere det eine utan det andre.

Ein fare ved å praktisere detaljert innsynslogging er at ho kan føre til at det blir trekt feilaktig negative slutningar som kan få konsekvensar for dei som figurerer i loggane. I personopplysningslova § 13 blir det stilt krav om at den behandlingsansvarlege skal sørgje for god nok informasjonstryggleik med omsyn til integriteten til opplysningane. Dette må òg reknast for å gjelde loggdata, og den behandlingsansvarlege pliktar slik sett å sikre integriteten til loggen. Dersom ein trekkjer konklusjonar frå loggen åleine, kan det oppstå situasjonar der personar blir skulda for å ha «snoka» i dokument i situasjonar der dei for eksempel har fått munnleg fullmakt til å gjere det. Sjølv om innsynslogging er eit kontrolltiltak som klårt kan tillatast etter arbeidsmiljølova kapittel 9, er den mistenkjeleggjeringa som omfattande bruk av logging kan føre med seg, uheldig. Regjeringa meiner derfor at det er viktig å innføre gode rutinar for å verifisere loggdata og følgje opp mistenkjelege loggdata.

Plikta til innsynslogging kan ikkje gjelde utan unntak. Det er ikkje all informasjon ein treng loggføre av omsyn til personvernet, og overflødig informasjon bør ikkje loggast. Det er derimot viktig å få eit fullstendig bilete av kva handlingar som blir utførte i eit system. Det blir og utvikla stadig fleire program for såkalla «flagging» av bruksmønster som kan indikere mogleg snoking.

I helse- og omsorgssektoren har ein eigne reglar for innsynslogging og innsyn i loggar. Sjå nærmare omtale i meldinga.

8.1.6.1 Innsyn i loggar som handlar om aktivitet knytt til eigne opplysningar

Det blir i meldinga peikt på at det at den registrerte skal få innsyn i eigne personopplysningar, er eit viktig personvernprinsipp. Etter personopplysnings-

lova § 18 har kvar den som ber om det, rett til å få innsyn i behandlinga av personopplysningar om seg sjølv og omstenda rundt denne behandlinga. Dette bør òg gjelde for innsynsloggane i ulike register.

Det blir i meldinga peikt på at det er viktig at kvar einskild blir informert om retten til å få innsyn i innsynsloggane til dei registera der han eller ho er oppført.

Det framgår vidare at ein viktig føresetnad for at innsynsretten skal kunne praktiserast, er at loggføringa er presis, og at den informasjonen som ligg i loggane, har god integritet.

Vidare blir det peikt på at ein må vurdere om den registrerte skal få innsyn i heile loggen eller berre dei delane av loggen som er viktige for at han eller ho skal kunne nytte rettane sine. Det viktigaste i denne samanhengen er at omfanget av innsyn i loggane skal vere tilstrekkeleg til at den registrerte kan få brukt rettane sine på ein god måte. Det er likevel mykje som talar for at innsynsretten i dei ulike registera bør vere så lik som mogleg, slik at dei registrerte opplever at dei har den same innsynsretten uavhengig av kva register det dreiar seg om.

8.1.6.2 Logging i større offentlege og private register

Det blir i meldinga vist til at logging er spesielt viktig i dei store registera der ein behandlar sensitive personopplysningar. I meldinga er omtale av nokre av sektorane der det er spesielt viktig å praktisere innsynslogging på ein god måte.

Eit område der ein har vedteke å utvide graden av innsynslogging, er registera til politiet. I den nye politiregisterlova er det vedteke eit krav om at opplysningane skal kunne sporast. Kravet inneber at opplysningar om bruk av systemet skal lagrast i eitt til tre år.

I samband med avgjerda om å modernisere arbeids- og velferdsetaten er det sett i gang ei omfattande modernisering av datasystema til etaten, mellom anna system for tilgangskontroll. Etaten har allereie etablert system for logging. Datatilsynet har derimot påpeikt at sikringa av fortrulegskap gjennom tilgangsstyring og logging ikkje er god nok. Nav arbeider for tida med å møte desse utfordringane, og dette er under evaluering av både Riksrevisjonen og Datatilsynet.

I finanssektoren er det òg viktig med logging. Både finansverksemder og forsikringsverksemder treng konsesjon frå Datatilsynet for å kunne behandle personopplysningar. Etter at konsesjonsvilkåra for bankar og finansinstitusjonar vart omgjorde våren 2010, vart det mellom anna innført strengare krav til korleis finansverksemdene skal praktisere tilgangskontroll og logging. Det vart òg avgjort at ein skulle gi kundane rett til innsyn i logg over elektroniske oppslag. Dei nye vilkåra inneber at dei elektroniske oppslaga tilsette gjer i personopplysningar skal loggast og lagrast i minst tre månader, og at kundane skal få innsyn i kor mange elektroniske oppslag tilsette har gjort, og når dei gjorde det. På grunn av implikasjonane dei «nye» vilkåra for mellom anna logging og innsyn i loggar fekk for IKT-systema til bankane, vart implementeringsfristen for desse vilkåra utsett, først til 1. juli 2012 og seinare til 31. mai 2013.

Forsikringsverksemder har eigen konsesjon frå Datatilsynet. Forsikringsselskap behandlar mange og sensitive opplysningar om kundane sine, og dei har svært omfattande register. Ein bør vurdere om det bør stillast liknande vilkår om logging og utvida innsyn til forsikringsverksemder som til finansverksemder.

8.1.6.3 Utgreiing om praktisering av logging og innsyn i loggar

I samband med stortingsbehandlinga av forslaget om å implementere datalagringsdirektivet i norsk rett bad Stortinget i Innst. 275 L (2010–2011) punkt 12, jf. vedtak nr. 473 11. april 2011, regjeringa om å drøfte desse spørsmåla i meldinga til Stortinget om personvern:

1. Kva avgrensingar som bør gjerast i loggplikta.
2. Retten til innsyn i loggar og omfanget av innsynet i kvart enkelt forhold.
3. Framdrifta i arbeidet med å verkeleggjere prinsippet om loggplikt og innsynsrett.

Å kartleggje praktiseringa av logging og innsyn i loggar i dei store registera, og særleg dei som inneheld sensitive personopplysningar i helse- og omsorgssektoren, finanssektoren, hos politiet og i Arbeids- og velferdssektoren, er eit omfattande arbeid.

På grunn av uvissa om kva praksis som gjeld i ulike sektorar og verksemder, er det svært vanskeleg å kome med konkrete tilrådingar om korleis loggplikta og innsynsretten i loggar bør avgrensast. Derfor har regjeringa bestemt at det skal setjast ned ei arbeidsgruppe som skal kartleggje praktiseringa av logging og innsyn i loggar i dei store offentlege og private registera, særleg dei som inneheld sensitive personopplysningar. På grunnlag av funna dei gjer, skal gruppa utarbeide retningsliner for praktisering av logging og innsyn i dei sektorane det gjeld. Arbeidsgruppa skal leiast av Fornyings-, administrasjons- og kyrkjedepartementet og ha medlemer frå dei departementa arbeidet gjeld.

8.1.7 Hovudpunkt kapittel

- Det bør fastsetjast eit prinsipielt mål om innebygd personvern i alle sektorar.
- Dei førehandsdefinerte standardinnstillingane på utstyr, i system og i program bør setjast til den mest personvernvenlege løysinga.
- Det bør leggjast til rette for sikker og forutsigbar bruk av nettskytenester innanfor rammene av det norske regelverket, blant anna ved å utarbeide rettleiingar.
- Der samtykke blir brukt som heimelsgrunnlag for behandling av personopplysningar, bør ein unngå tekniske løysingar for innhenting av samtykke som grensar mot implisitt samtykke eller ei form for reservasjonsrett.
- Det skal setjast ned ei interdepartemental arbeidsgruppe som skal greie ut klientbasert logging og retten til innsyn i desse loggane i dei større offentlege og private registera.

8.2 Komiteens merknader

Komiteen viser til at personopplysninger i stadig større grad er blitt en handelsvare. Det er vesentlig at norsk rett løpende tilpasses rettsutviklingen i våre naboland og i EU. Komiteen mener det vil bli nødvendig å vurdere begrensninger av videresalg av opplysninger. Bare hvis landene står sammen, kan man ha håp om å påvirke multinasjonale aktører som Facebook og Google. Både kontroll med tilgang og innsynslogging er vesentlige virkemidler i dette arbeidet.

Komiteens medlemmer fra Fremskrittspartiet, Høyre og Kristelig Folkeparti viser til at mens det tidligere var lagret personlige opplysninger på den enkelte pc, skjer det nå i større grad opplasting og lagring på nett. Et ledd i denne utviklingen er Cloud Computing (Nettsky). Det er et stort informasjonsbehov som må dekkes hos konsumentene som gjør at de kan ta stilling til sikkerhetspolicy, hvilken lokalisering serverne har, og hvilken kontroll de da vil ha med opplysningene som lagres.

Disse medlemmer ville anse det som et fremskritt for personvernet hvis prinsippet om informert samtykke også var en betingelse for bruk av «cookies», tekststrenger som husker hvilke sider som er besøkt på nettet, og som senere kan aktiveres for individualiserte henvendelser, for eksempel reklame.

9. Personvernstyremakta – organisering og oppgåver

9.1 Sammendrag

9.1.1 Innleiing – oppgåver og verkemiddel, status i andre land

Det blir i meldinga vist til at Datatilsynet er den sentrale personvernstyremakta. Tilsynet vart oppretta i 1980 og har vakse frå ei verksemd med nokre få tilsette til om lag 40 i dag. Verksemda er inndelt i fire avdelingar: administrasjonsavdelinga, kommunikasjonsavdelinga, juridisk avdeling og tilsyns- og tryggleiksavdelinga.

Oppgåvene til tilsynet er definerte i personopplysningslova § 42.

Datatilsynet fører i tillegg tilsyn etter ulike lover.

Datatilsynet har definert følgjande som kjerneoppgåvene sine:

- Behandle innkomne saker og drive tilsynsverksemd, jf. personopplysningslova § 42 nr. 2 og 3.
- Gi råd og rettleiing til privatpersonar, næringsdrivande, offentlege etatar o.l., jf. personopplysningslova § 42 nr. 6.
- Vere ombod for personvernspørsmål, jf. personopplysningslova § 42 nr. 5.
- Drive informasjonsarbeid, jf. personopplysningslova § 42 nr. 5 og 6.

Dette samsvarar langt på veg med omtalen Personvernkommisjonen har gitt, sjå rapporten frå kommisjonen, punkt 18.1.2.

Både tilsynsverksemd og informasjonsarbeid er verkemiddel Datatilsynet nyttar for å gjere personvernregelverket betre kjent. Ombodsrolla blir òg brukt aktivt som eit verkemiddel i samanhengar der tilsynsrolla anten ikkje fungerer godt, eller der det ikkje er rettsleg grunnlag for å bruke den kompetansen Datatilsynet har som tilsyn.

Datatilsynet er oppretta som eit uavhengig tilsynsorgan underlagt Fornyings-, administrasjons- og kyrkjedepartementet. NOU 1997:19 Et bedre personvern peikte bl.a. på at «departementets etatsstyring må ta hensyn til at tilsynsmyndigheten skal være faglig uavhengig».

At Datatilsynet skal vere uavhengig, er stadfesta i Ot.prp. nr. 92 (1998–1999) og i Innst. O. nr. 51 (1990–2000), der «komiteen er enig med Justis- og beredskapsdepartementets karakteristikk av Datatilsynet som et faglig uavhengig forvaltningsorgan med særskilt vide fullmakter». Den uavhengige stillinga er òg forankra i europeisk regelverk. I EUs forslag til forordning på personvernområdet er den uavhengige stillinga omtala i kapittel 6. Her blir alle EU/EØS-land pålagde å ha ei uavhengig personvernstyremakt.

Enkeltvedtaka til Datatilsynet kan likevel klagast inn til Personvernnemnda.

I tillegg arbeider ei lang rekkje tilsynsstyremakter med spørsmål knytte til behandling av personopplysningar på sitt kompetanseområde. Dette gjeld mellom anna Arbeidstilsynet, Post- og teletilsynet, Helsetilsynet og Forbrukarombodet.

Datatilsynsstyremaktene i EØS-området er ulikt organiserte. Eit gjennomgåande trekk er likevel at organa er organiserte som sjølvstendige sektorstyremakter, og at dei i tillegg til tilsynsoppgåver har ei ombodsrolle ved at dei skal skape medvit rundt og delta i debattar om personvern. Oppgåvene deira består i hovudsak av å behandle saker om og føre tilsyn med bruk av personopplysningar, gi rettleiing om behandling av personopplysningar og kome med høyringsfråsegner. Trass i noko ulike oppgåver er det relativt liten skilnad på korleis personvernstyremaktene i dei nordiske landa er organiserte, og det er godt samarbeid mellom etatane.

9.1.2 Hovudmoment i rapporten frå Personvernkommisjonen

Organiseringa av personvernstyremakta er omtala i kapittel 11 i rapporten frå Personvernkommisjonen. Personvernkommisjonen kjem med fleire forslag til endringar. Forslaga omhandlar desse tema:

– oppgåvene og ressursane til Datatilsynet
– regionalisering av Datatilsynet
– oppretting av eit råd for Datatilsynet
– sektorvis styring av personvernkompetansen
– dialog med akademia og andre fagmiljø

9.1.3 Hovudfunn i evalueringa til Difi

Hausten 2010 gav Fornyings-, administrasjons- og kyrkjedepartementet Direktoratet for forvaltning og IKT (Difi) i oppdrag å evaluere Datatilsynet. Evalueringa var ei oppfølging av framlegget frå Personvernkommisjonen. Målet med prosjektet var

– å vurdere om personvernstyremaktene, og Datatilsynet som hovudaktør, har dei nødvendige føresetnadane for å kunne oppfylle rollene og oppgåvene sine i samsvar med personopplysningslova
– å gi Fornyings-, administrasjons- og kyrkjedepartementet eit betre grunnlag for å vidareutvikle styringsdialogen mellom FAD, Datatilsynet og Personvernnemnda
– å gi Datatilsynet eit godt verktøy for framtidig organisasjons- og utviklingsarbeid

Som ein del av arbeidet vart ei rekkje interne og eksterne informantar intervjua.

Rapporten Evaluering av Datatilsynet vart framlagd 3. oktober 2011.

Hovudkonklusjonen til Difi var at Datatilsynet oppnår gode resultat på eit breitt område. Det vart òg understreka at Datatilsynet hadde utvikla seg positivt både med tanke på å gjere organisasjonen betre rusta til å løyse ulike typar oppgåver og til å kome i konstruktiv dialog med ulike målgrupper. Dei fleste informantane vurderte Datatilsynet som ein god rådgivar i personvernspørsmål, samstundes som det kom fram noko kritikk frå enkelte informantar som meinte Datatilsynet ikkje alltid er gode nok til å vurdere ulike omsyn mot kvarandre.

Det vart òg peikt på enkelte ting som kunne bli betre. Rapporten peikte mellom anna på behovet for meir strategisk bruk av verkemiddel og ressursstyring, sterkare rollemedvit, ei tydeleggjering av ombodsrolla, betre samarbeid med ulike målgrupper og betre forvaltningskompetanse.

Rapporten frå Difi konkluderer med at det er lite fagleg kontakt mellom Datatilsynet og Personvernnemnda. Datatilsynet er likevel bevisst på å bruke klageorganet for å få avklåra prinsipielle tolkingsspørsmål. Sidan Datatilsynet er eit fagleg uavhengig forvaltningsorgan, er den faglege kontakten mellom Datatilsynet på den eine sida og Justis- og beredskapsdepartementet og Fornyings-, administrasjons- og kyrkjedepartementet på den andre òg etter måten liten. Departementa er mellom anna varsame med å uttale seg om korleis regelverket skal tolkast, fordi bruk av reglane er ei oppgåve for Datatilsynet og eventuelt Personvernnemnda.

9.1.4 Datatilsynet – den nye arbeidsforma og den meir strategiske tilnærminga

For å leggje til rette for effektiv ressursbruk på alle område gjennomførte Datatilsynet ein intern strategiprosess parallelt med evalueringa til Difi. Den nye strategien vart lansert i november 2011 og peiker ut kva retning Datatilsynet skal gå i dei neste fem åra.

Eit hovudpunkt her er ei meir strategisk arbeidsform. Datatilsynet vedtek kvart år ein detaljert verksemdsplan som slår konkret fast kva aktivitetar etaten skal gjennomføre. I tillegg har Datatilsynet vedteke fagstrategiar på helseområdet, i justissektoren og på det internasjonale området.

Eit anna viktig punkt i strategien er å medverke til auka interesse for og kunnskap om personvern og vidare å arbeide for at andre aktørar òg legg vekt på personvern.

Strategien legg òg vekt på kor viktig det er med kvalitet og kompetanse. Det er sett i gang ein plan for å heve kompetansen internt. Datatilsynet gjer òg i større grad enn tidlegare klåre prioriteringar av innkomne saker og har som mål å behandle fleire saker

ved å gi rettleiing framfor å gi kvar sak ei full forvaltningsbehandling.

Til slutt er det ei viktig oppgåve å identifisere farar for personvernet og vere synleg og tydeleg i den offentlege debatten. Datatilsynet skal bruke ombodsrolla til å fremje debatt, men samtidig markere tydeleg i kvart einskilt tilfelle kva for ei av rollene sine etaten spelar.

9.1.5 Datatilsynet framover

9.1.5.1 Bør Datatilsynet drive både tilsynsverksemd og ha rolla som ombod for personvernspørsmål?

Det er ikkje uvanleg i norsk forvaltning at eit organ har fleire roller. Det er likevel ikkje vanleg med to så tydelege roller i eitt og same organ som det ein finn i Datatilsynet. Både Difi og Personvernkommisjonen peiker på at det kan vere krevjande å ha rolla som både tilsyn og ombod. Medan tilsynsrolla krev nøytralitet og objektivitet, ligg det i rolla som ombod at ein skal ta konkret stilling til ulike spørsmål. Difi peiker i rapporten på at det sterke engasjementet blant dei tilsette i etaten kan føre til at medvitet om rolla som forvaltningsorgan ikkje alltid er sterk nok. Datatilsynet sjølv peiker i strategien sin på at det kan vere spesielt krevjande å skilje mellom dei to rollene når ein går frå ombodsrolla til tilsynsrolla.

Difi peiker i evalueringa av Datatilsynet på ei oppfatning av at tilsynet ikkje alltid godt nok veger omsyn og regelverk opp mot kvarandre, og at dei i for stor grad einsidig legg vekt på personvernomsyn. I evalueringa frå Difi er det òg lagt vekt på at hovudtyngda av informantane viser stor forståing for dei ulike rollene Datatilsynet har, og meiner at etaten i hovudsaka balanserer bra i arbeidet med ulike oppgåver.

Det er mange fordelar med å kombinere dei to rollene, som i mange tilfelle overlappar kvarandre. I høyringsarbeidet glir rollene over i kvarandre. I informasjonsarbeidet er det òg vanskeleg å skilje mellom informasjon som blir gitt i rolla som ombod, og informasjon som blir gitt i rolla som tilsyn. Som tilsyn får Datatilsynet kvart år ca. 10 000 meldingar og telefonsamtaler frå næringsdrivande og privatpersonar. Datatilsynet kan derfor basere synspunkta sine i høyringssaker og utvalsarbeid på ein unik og erfaringsbasert kunnskap om korleis personvernlovgivinga faktisk blir etterlevd.

Ein kombinasjon av dei to rollene gir dessutan Datatilsynet eit større handlingsrom enn om rollene var skilde.

Aktivt internasjonalt engasjement er viktig for Datatilsynet. Eit eventuelt reint ombod på personvernområdet vil ikkje ha tilgang til dette nettverket.

Det blir i meldinga vist til at for sterk oppsplitting i forvaltningsorgan med reindyrka roller vil kunne gi ei uoversiktleg forvaltning. I samband med evalueringa av Datatilsynet peiker Difi likevel på at det kan vere nødvendig å avklåre ombodsrolla til statlege organ meir generelt. I Datatilsynet sitt tilfelle verkar fordelane med å halde på begge rollene først og fremst å vere at etaten i utøvinga av ombodsrolla kan dra nytte av den verdifulle informasjonen og kompetansen dei opparbeider seg gjennom å utøve rolla som tilsynsstyremakt. For eit lite organ som Datatilsynet med eit stort arbeidsfelt er dette svært verdifullt. Den største utfordringa ved å kombinere dei to rollene er at det kan vere krevjande både for tilsynet sjølv og for dei som samhandlar med tilsynet, å vite kva rolle etaten til kvar tid opptrer i, og dermed kva verkemiddel dei kan bruke.

I Datatilsynet sitt tilfelle meiner regjeringa at fordelane med å halde dei to rollene i eitt og same organ skyggjer over ulempene. Regjeringa viser òg til at fleirtalet i Personvernkommisjonen – 14 medlemer – meiner at kombinasjonen av roller i Datatilsynet bør vidareførast. Dette er òg den konklusjonen regjeringa har trekt. Samtidig blir det understreka at det er viktig at Datatilsynet er tydeleg på dei ulike rollene sine, og spesielt når det flytter seg frå ombodsrolla over i tilsynsrolla. Datatilsynet har i det store og heile klart å balansere dei to rollene på ein tilfredsstillande måte, noko som òg blir understreka i evalueringsrapporten frå Difi. Det blir lagt til grunn at Datatilsynet òg i det vidare arbeidet arbeider aktivt med rolleforståinga, slik at det blir mogleg å kombinere dei to rollene på ein god måte. Det er viktig å ha eit sterkt, synleg og uavhengig datatilsyn som fremjar personvernomsyn og talar personvernet si sak.

9.1.5.2 Om dialog med forskings- og utviklingsmiljø

Både Difi og Personvernkommisjonen har peikt på kor viktig det er at Datatilsynet har kontakt med forskings- og utviklingsmiljø. Ein del av den strategiske satsinga til Datatilsynet går ut på å styrkje dialogen med FoU-miljøa og setje i verk forskingsprosjekt på personvernområdet. Datatilsynet har òg eit etablert samarbeid med fleire høgskular og universitet. Regjeringa legg derfor til grunn at Datatilsynet held fram med å utvikle forholdet til forskings- og utviklingsmiljøa til felles nytte.

9.1.5.3 Eit råd for Datatilsynet

Personvernkommisjonen føreslår at det blir oppretta eit «Datatilsynets råd», som kan fungere som «et kollektivt rådgivningsorgan med bredere sammensetning enn man finner i Datatilsynets profesjonelle stab». Dette er grunngitt med at personopplysningslova krev mange interesseavvegingar, og at ein bør sikre at det også blir lagt vekt på andre interesser enn personverninteressene.

Det går fram av meldinga at det ikkje er aktuelt no å opprette eit råd for Datatilsynet, slik Personvernkommisjonen har teke til orde for. Dersom enkeltsaker, rapportar og tilsynsrapportar skal leggjast fram for eit kollegialt råd, vil det mest truleg føre til lengre saksbehandlingstid enn i dag. Datatilsynet har stor sakspågang, og eit råd kan derfor lett bli eit kompliserande og fordyrande ledd i saksbehandlinga. Personvernnemnda har i dag full kompetanse til å overprøve enkeltvedtaka Datatilsynet gjer. Eit råd vil i mange tilfelle føre til at det i realiteten kan bli tre instansar som vurderer saker. Godt samarbeid og god dialog med sektorinteresser, næringsliv og andre styremakter kan tilføre Datatilsynet informasjon som legg grunnlag for ei balansert saksbehandling, og kan dermed redusere behovet for eit rådgivingsorgan.

I forslaget til ny EU-forordning blir det understreka at tilsynsstyremakta skal vere absolutt uavhengig.

Personvernkommisjonen peiker på at personopplysningslova krev breie vurderingar og interesseavvegingar. Datatilsynet vil, ved å satse på kompetanseutvikling og auka kontakt med ulike målgrupper og FoU-miljø, vere godt rusta til å gjere dei avvegingane fagområdet krev. I klagesaker blir desse vurderingane tekne av Personvernnemnda.

9.1.5.4 Samarbeid med eksterne aktørar

Difi understrekar i rapporten sin (kapittel 7.2) kor viktig det er at Datatilsynet gjer ei strategisk vurdering av den samla verksemda og bruken av verkemiddel, medrekna samarbeid med eksterne aktørar.

Omfattande kontakt med eksterne aktørar er ei viktig strategisk satsing for Datatilsynet. Det er viktig med slik kontakt, og det synest å vere ein situasjon alle partar tener på. Gjennom aktiv rådgiving kan Datatilsynet bidra til at eksterne aktørar tek omsyn til personvernet i si eiga verksemd. Som Difi peiker på, er det likevel viktig å formidle klårt kvar grensa går for kva Datatilsynet skal bidra med. Dette er viktig av ressursomsyn, men òg for å sikre eigen nøytralitet.

Regjeringa vil dessutan understreke kor viktig det er at Datatilsynet legg vekt på å ha kontakt med eksterne aktørar – både næringsliv, interesseorganisasjonar og andre instansar – og på den måten opparbeide betre sektorkompetanse og forståing for utfordringane i sektoren. Dette vil gjere tilsynet endå betre i stand til å ta dei breie avvegingane feltet krev.

9.1.5.5 Datatilsynet – arbeidsformer, effektivisering og prioriteringar

Difi nemner i punkt 7.7 i evalueringsrapporten sin at mange informantar meiner ein bør effektivisere den daglege saksbehandlinga i Datatilsynet. Som Difi òg peiker på, har Datatilsynet vurdert korleis saksbehandlinga kan organiserast, og kva saker som spesielt skal prioriterast. Datatilsynet har òg nyleg lansert ei ny nettside, og det er eit mål at heimesida skal gi svar på dei spørsmåla eit informasjonssøkjande publikum er oppteke av.

Det blir i meldinga vist til at det ikkje er grunn til å tru at saksmengda til Datatilsynet kjem til å bli mindre i åra framover og at det derfor er viktig at tilsynet stadig arbeider for å effektivisere arbeidsmetodane sine.

9.1.5.6 Kompetansen til Datatilsynet

Både Personvernkommisjonen og Difi understrekar at det er viktig at Datatilsynet har ein breitt samansett kompetanse.

I strategien til Datatilsynet er høg kompetanse ei av dei viktigaste strategiske satsingane, i tillegg til brei kontakt med eksterne aktørar. Det er laga ein plan for å heve kompetansen internt.

Regjeringa vil understreke behovet for at eit sektorovergripande tilsyn har god sektorkompetanse. Det er Datatilsynet som sjølv må vurdere korleis kompetansen skal vere samansett internt. Det er likevel viktig å understreke kor mykje det har å seie at Datatilsynet har god teknologisk kompetanse. God internasjonal kompetanse gjer det lettare å få gjennomslag i internasjonale forum, og derfor blir òg slik kompetanse vurdert som spesielt viktig.

9.1.5.7 Regionalisering av Datatilsynet

Personvernkommisjonen meiner Datatilsynet bør regionaliserast, og føreslår å opprette fleire regionkontor. Føremålet er å få ei meir lokal forankring i personvernarbeidet.

Personvernkommisjonen går inn for at eit eventuelt regionapparat bør ha minst seks tilsette på kvart kontor for at kontora skal bli effektive. Regjeringa er einig i at eventuelle regionkontor må ha ei viss minimumsbemanning. Regionkontor med ei bemanning i samsvar med forslaget frå Personvernkommisjonen ville derimot ha ført til nesten ei dobling av talet på tilsette i personvernstyremakta. Regjeringa ser ikkje føre seg at Datatilsynet i åra som kjem bør styrkjast i eit omfang som kan rettferdiggjere ein slik vekst i regionane. Så synleg og kompetent som Datatilsynet er i dag, vil ei oppsplitting av etaten gjennom å etablere regionkontor i stor grad kunne setje personvernarbeidet tilbake, i alle fall på mellomlang sikt. Mykje talar for at så små fagmiljø som dei offentlege personvernmiljøa ikkje er tente med ei oppsplitting i regionkontor. Regjeringa går derfor inn for å halde ved lag eit sentralisert datatilsyn etter den eksisterande modellen.

9.1.5.8 Ressursbehovet til Datatilsynet i åra som kjem

Personvernkommisjonen meinte at Datatilsynet har for små ressursar i høve til dei omfattande oppgåvene tilsynet er tildelt. Kommisjonen føreslo at Datatilsynet skal få større ressursar, og at dei spesielt må bruke ressursane til å styrkje kompetansen på informasjonsteknologi.

Det blir i meldinga peikt på at samanlikna med dei nordiske systerorganisasjonane er ressurssituasjonen til Datatilsynet også relativt bra. Datatilsynet har dessutan dei seinare åra fått noko auka løyvingar, mellom anna som følgje av nye tilsynsoppgåver, no sist etter ekomlova og politiregisterlova.

Samtidig ser regjeringa at det dukkar opp stadig fleire og meir komplekse problemstillingar knytte til personvern. Datatilsynet har ei stor saksmengd. Det er viktig at Datatilsynet er aktivt til stades på den internasjonale arenaen, noko som òg er ressurskrevjande. Regjeringa har vurdert at dei omfattande oppgåvene tilsynet har fått som følgje av at datalagringsdirektivet skal implementerast i norsk rett, og som følgje av den nye politiregisterlova, kan tilseie at løyvingane bør aukast noko, slik at tilsynet blir i stand til å gi nødvendig rettleiing og føre tilfredsstillande tilsyn på dette området. I Prop. 1 S (2012–2013) er det føreslått å auke budsjettet til Datatilsynet for 2013 med drygt 1,7 mill. kroner i høve til 2012-budsjettet for å setje tilsynet i stand til å ta seg av desse oppgåvene.

9.1.5.9 Sektorvis styrking av personvernkompetansen

Personvernkommisjonen føreslår å styrkje personvernkompetansen sektorvis ved at andre organ som får med personvernspørsmål å gjere, bør ha ein person internt med høg kompetanse på personvernspørsmål. Det er føreslått at dette først og fremst blir gjort gjennom å opprette personvernombod i desse organa.

Regjeringa er einig med kommisjonen i at organ som ofte har med personvernspørsmål å gjere, bør ha spesiell kompetanse på området.

Regjeringa vil sjå spørsmålet om sektorvis styrking av personvernet i samanheng med utviklinga av personvernombodsordninga. Det er likevel viktig å understreke at sektorvis styrking av personvernkompetansen må vurderast breiare enn til berre å gjelde oppretting av personvernombod. I strategien til Datatilsynet er eit av satsingsområda å medverke til større interesse for personvern og arbeide for at også andre legg vekt på personvernomsyn i arbeidet. Regjeringa har òg over tid arbeidd for betre personvernarbeid på dei ulike fagområda, mellom anna ved å utarbeide ei rettleiing i vurdering av personvernkonsekvensar til bruk i utgreiingsarbeidet i forvaltninga. Det blir i meldinga vist til at desse tiltaka, saman med at Datatilsynet har systematisk kontakt med sentrale aktørar i den offentlege forvaltninga og i næringslivet, kan medverke til at andre sektorar legg større vekt på personvern.

9.1.6 Særleg om ordninga med personvernombod

Ordninga med personvernombod er i dag frivillig. Det er no om lag 200 personvernombod fordelte på i underkant av 400 verksemder i både offentleg og privat sektor. Somme ombod hjelper fleire behandlingsansvarlege utan å vere tilsette hos nokon av dei. Andre personvernombod er tilsette i verksemda og har oppgåva som personvernombod på fulltid. Dei blir omtala som personvernombod, sjølv om dei kanskje betre kan omtalast som personvernrådgivarar, sidan meininga er at hovudoppgåva skal vere å gi råd både til behandlingsansvarlege og registrerte. Det er òg teke omsyn til dette i den nye politiregisterlova, der ordninga med personvernrådgivarar er lovfesta.

Ordninga med personvernombod er i dag berre laust forankra i norsk personopplysningsregelverk og i EUs personverndirektiv. Reguleringa er i hovudsak relatert til lemping eller forenkling av meldeplikta for behandling av personopplysningar hos behandlingsansvarlege som har oppretta personvernombod. Det finst ikkje reglar i norsk lov eller forskrift som direkte regulerer oppgåvene og ansvaret til omboda, og heller ikkje reglar om kva plikter og ansvar den behandlingsansvarlege har overfor omboda. Eit forslag om klårare regelfesting og regulering av ordninga ligg til vurdering i Justis- og beredskapsdepartementet som eit ledd i etterkontrollen av personopplysningslova. Eit av forslaga er å lette på fleire av pliktene til den behandlingsansvarlege dersom det blir oppretta personvernombod. Slike lettar i pliktene etter regelverket føreset at personvernomboda er godt skolerte og har ei sterk stilling i høve til den behandlingsansvarlege. I motsett fall kan oppretting av eit personvernombod bli ei sovepute. Eventuelle endringar i ordninga med fleire oppgåver for ombodet og færre plikter for den behandlingsansvarlege må derfor vurderast nøye.

Etter forslaget til ny personvernforordning i EU skal alle offentlege organ og private verksemder med over 250 tilsette ha personvernombod («data protection officer»).

Den norske ordninga med personvernombod vart evaluert i 2011 då Synnovate gjennomførte ei spørjeundersøking blant personvernomboda, leiarar og tilsette i verksemder med ombod. Resultata frå undersøkinga er sprikande.

I Difi-evalueringa av Datatilsynet vart det òg stilt spørsmål om ordninga med personvernombod. Svara i undersøkinga Difi har gjort, er med på å underbyg-

gje dei noko sprikande svara om effekten av ordninga som kom fram i undersøkinga Synnovate utførte.

I stortingsbehandlinga av forslaget om å implementere datalagringsdirektivet i norsk rett bad Stortinget i oppmodingsvedtak nr. 473 11. april 2011 regjeringa om å leggje Innst. 275 L (2010–2011) til grunn for det vidare arbeidet. I punkt 12 g vart regjeringa beden om å sørgje for å etablere ei ordning med personvernrådgivarar/-koordinatorar i større statlege etatar som behandlar sensitive personopplysningar, spesielt Arbeids- og velferdsforvaltninga og helsesektoren. Å opprette ein funksjon som personvernrådgivar, slik politiregisterlova legg opp til i politiet, vil vere eit nyttig tiltak for å rette søkjelyset mot personvernspørsmål. Samtidig viser evalueringa av ordninga med personvernombod at det er noko usikkert kva verknad omboda faktisk har på personvernnivået hos den behandlingsansvarlege. Eit pålegg om å opprette personvernrådgivarar/-koordinatorar i visse sektorar og hos visse behandlingsansvarlege krev derfor at ein klårgjer og regelfestar innhaldet i ordninga i langt større grad enn det som i dag er tilfellet.

EUs utkast til personvernforordning vil, slik forslaget ligg føre, leggje sterke føringar på korleis ein skal utforme ordninga med personvernrådgivarar. Dersom det endelege EU-regelverket regulerer ordninga, må desse reglane mest truleg òg innførast i Noreg. Regjeringa ser det slik at ei ordning med personvernrådgivarar i store verksemder som behandlar sensitive personopplysningar, kan vere eit godt tiltak for å rette søkjelyset mot personvern i verksemda og på den måten styrkje regeletterlevinga. Rådgivaren kan gjere sitt til å betre personvernet for dei registrerte. Regjeringa ønskjer å vente med ei ny regulering av ordninga med personvernrådgivarar/personvernombod og nye pålegg om å etablere personvernrådgivarar til EUs personvernregelverk er ferdig revidert, og til det eventuelt er vedteke klårare reglar for korleis personvernrådgivarane skal vere organiserte og forankra i verksemda, og kva oppgåver dei skal ha.

Regjeringa ønskjer likevel å presisere at både offentlege og private verksemder som behandlar store mengder av personopplysningar, kan vere tente med å ha god lokal personvernkompetanse. Desse verksemdene står fritt til å etablere personvernombod i tråd med tilrådingar frå Datatilsynet, eventuelt personvernrådgivarar med oppgåver som verksemda sjølv definerer, med det føremålet å betre regeletterlevinga og det generelle personvernet i verksemda. Mange av dei store helseføretaka har òg etablert personvernombod/personvernrådgivarar, noko regjeringa ser på som positivt. Dersom EU vedtek endringar i personvernreguleringa, vil det vere naturleg for regjeringa å gå gjennom og revidere den norske ordninga med personvernombod/-rådgivar i lys av den internasjonale reguleringa.

9.1.7 Personvernnemnda

Personvernnemnda er klageorgan for vedtak Datatilsynet har gjort i medhald av personopplysningslova eller anna regelverk tilsynet har vedtakskompetanse etter. Nemnda har sju medlemer med personlege varamedlemer.

Personvernnemnda er eit fagleg uavhengig forvaltningsorgan. Ved at klagesaker blir behandla i nemnda, og ikkje som tidlegare i departementet, er tilsynsstyremakta sikra ei uavhengig stilling, slik det er nedfelt i EUs personverndirektiv og personopplysningslova. Nemnda er samansett på ein slik måte at ho er godt rusta til å gjere vurderingar i saker der personvern er eitt av fleire moment som skal vurderast. Tradisjonelt har nemnda derfor hatt både teknologisk, økonomisk og medisinsk kompetanse i tillegg til juridisk kompetanse.

Saksmengda i Personvernnemnda har variert noko sidan nemnda vart oppretta, men har dei seinaste åra lege på om lag 10–15 saker per år.

Om lag halvparten av vedtaka i Datatilsynet som blir innklaga til nemnda, blir omgjorde. Omgjeringsprosenten i høve til kor mange vedtak Datatilsynet gjer, er likevel svært låg, sidan under 5 pst. av vedtaka i Datatilsynet blir sende inn til Personvernnemnda til klagesaksbehandling.

Personvernnemnda er eit reint klageorgan og gjer vedtak som berre er bindande for partane i kvar einskild sak. Det er svært sjeldan saker på personvernområdet blir klaga inn til behandling i rettsapparatet. Sidan Personvernnemnda er klageorgan på personvernområdet, har vedtaka nemnda gjer, stor presedensverknad i andre og tilsvarande saker som kjem til behandling i Datatilsynet. Det er derfor viktig at vedtaka nemnda gjer, blir skrivne på ein måte som gjer dei eigna til å bli brukte som rettleiing i liknande saker seinare.

Regjeringa meiner ordninga med ei uavhengig klagenemnd på personvernområdet til no har fungert godt. Også ordninga med at utnemninga av medlemene i nemnda er delt mellom Stortinget og regjeringa, meiner regjeringa fungerer godt. Regjeringa har vurdert om det er grunnlag for å endre ordninga med personlege varamedlemer, vurderer det inntil vidare som føremålstenleg å halde Personvernnemnda ved lag med personlege varamedlemer i den noverande forma.

9.1.8 Fornyings-, administrasjons- og kyrkjedepartementet og Justis- og beredskapsdepartementet

I regjeringa er hovudansvaret for det generelle arbeidet med personvernsaker delt mellom Fornyings-, administrasjons- og kyrkjedepartementet og Justis- og beredskapsdepartementet. Justis- og beredskapsdepartementet har ansvaret for personopplys-

ningslova og følgjer opp arbeid med personvern både i Europarådet og EU. Fornyings-, administrasjons- og kyrkjedepartementet har ansvaret for personopplysningsforskrifta, etatsstyringa av Datatilsynet og Personvernnemnda og dessutan for det generelle personvernarbeidet til regjeringa. Fornyings-, administrasjons- og kyrkjedepartementet deltek òg i personvernarbeidet i regi av OECD. Før personopplysningslova vart vedteken, låg heile ansvaret for personvernområdet hos Justisdepartementet. Det administrative ansvaret for Datatilsynet vart flytt til Arbeids- og administrasjonsdepartementet i 2000 for å sikre at etatsstyringa av Datatilsynet ikkje skulle kome i konflikt med interessene til Justis- og beredskapsdepartementet som etatsstyrar av fleire store behandlingsansvarlege.

Arbeidsfordelinga mellom departementa fungerer bra.

Det ligg ikkje føre konkrete planar om å endre den noverande arbeidsfordelinga på personvernområdet.

9.1.9 Hovudpunkt kapittel 9

- Datatilsynet er ein relativt liten organisasjon med avgrensa ressursar og eit omfattande arbeidsområde.
- Datatilsynet bør vere tydeleg på når det opptrer som ombod, og når det opptrer som tilsyn.
- Det blir ikkje lagt opp til endringar i organiseringa av Datatilsynet. Etaten bør ha merksemd retta mot organisasjonsutvikling og rekruttering av ulike typar kompetanse og leggje vekt på å ha god kontakt med ulike fag- og forskingsmiljø.
- Ordninga med personvernombod som er utvikla av Datatilsynet, har vakse mykje dei siste åra. Før nokon blir pålagd å etablere personvernombod/personvernrådgivar, må ein få på plass ei klårare rettsleg forankring og regulering av ordninga, noko som må sjåast i lys av endringar i internasjonalt regelverk på området.
- Klageorganet Personvernnemnda gjer om vedtak frå Datatilsynet i om lag halvparten av dei sakene nemnda får til behandling. Talet på klager over vedtaka til Datatilsynet er likevel svært lågt sett i høve til kor mange vedtak tilsynet gjer totalt.

9.2 Komiteens merknader

Komiteen er opptatt av Datatilsynets uavhengighet innenfor de rammer som er trukket opp av Stortinget i lovs form.

Komiteens medlemmer fra Fremskrittspartiet, Høyre og Kristelig Folkeparti vil peke på at Datatilsynet og Personvernnemnda er blitt vurdert av Difi, som har utarbeidet en rapport om virksomheten, der man finner at tilsynet fyller sine funksjoner både som ombud og tilsynsorgan for førstnevnte og nemnda som klageorgan, på en god måte, og at dette oppnås innenfor en moderat ressursramme.

Disse medlemmer deler synspunktet på at organiseringen så langt har vært hensiktsmessig, og derfor ikke tilsier noe behov for endringer.

Disse medlemmer vil understreke at statens egne forvaltningsledd, sentraladministrasjon så vel som statlige foretak, forutsettes å rette seg etter Datatilsynets og Personvernnemndas avgjørelser.

Disse medlemmer tar til etterretning at regjeringen ikke støtter forslaget fra Personvernkommisjonen om en viss regionalisering av Datatilsynet for å utvide tilsynsfunksjonen. Derimot vil det lokale personvernarbeidet kunne bli påvirket av EUs forslag til personvernforordning, som setter krav til bedrifter med mer enn 250 ansatte om å ha en personvernrådgiver.

10. Økonomiske og administrative konsekvensar

10.1 Sammendrag

Det blir i meldinga tilrådd ulike generelle løysingar og tiltak for så god ivaretaking av personvernet som råd.

Personvernvenlege løysingar kan vere dyrare enn mindre gode løysingar. Innkjøpskostnadene kan dermed vere noko høgare ved val av løysingar som tek hand om personvernomsyn og prinsippa i denne meldinga på ein god måte, og som gjer at ein står betre rusta til å oppfylle personvernvilkåra i eksisterande regelverk. Det er likevel å vente at dersom ein legg til grunn dei prinsippa som meldinga held fram, kjem dei som behandlar personopplysningar, til å utvikle rutinar og system som på sikt effektiviserer behandlinga av personopplysningar og lettar regeletterlevinga. Kor stor innsparinga kan bli, kan variere frå sektor til sektor, avhengig av mellom anna kva personopplysningar som blir behandla, og kva høve det er til effektivisering.

Effekten av tiltaka kan liggje eit stykke fram i tid, utan at det er råd å seie nøyaktig når han kjem. Kostnader ved val av personvernvenlege løysingar er eitt av fleire moment som må ha vekt når ein skal velje. Desse kostnadene må i kvart einskilt tilfelle dekkjast av den verksemda som skal gjere innkjøpet.

Å endre eksisterande system så dei blir meir personvernvenlege, kan vere kostbart. Det blir ikkje lagt opp til at eksisterande system skal endrast for å oppfylle tilrådingane i denne meldinga.

I meldinga blir det på fleire område lagt opp til å utarbeide rettleiingar og/eller informasjonsmateriell som skal leggje til rette for betre regeletterleving på

personvernområdet. Kostnadene ved å utarbeide slikt materiell blir dekte innanfor dei vanlege budsjettrammene til Fornyings-, administrasjons- og kyrkjedepartementet og Datatilsynet. Når slike rettleiingar ligg føre, er dei med og lettar regeletterlevinga, og det fører venteleg til både administrative og økonomiske fordelar for dei behandlingsansvarlege på sikt.

Kostnader ved deltaking i internasjonalt personvernarbeid blir dekte innanfor dei vanlege budsjettrammene til departementa og dei underliggjande etatane.

10.2 Komiteens merknader

K o m i t e e n har ingen merknader.

11. Forslag fra mindretall

Forslag fra Fremskrittspartiet, Høyre og Kristelig Folkeparti:

Forslag 1

Stortinget ber regjeringen gjennomgå implikasjonene av utvidelsene av den svenske FRA-loven og fremme en sak til Stortinget om hvordan man kan sikre at innbyggere i Norge får bedre beskyttelse i sin tele- og datakommunikasjon.

12. Komiteens tilråding

K o m i t e e n har for øvrig ingen merknader, viser til meldingen og rår Stortinget til å gjøre slikt

v e d t a k :

Meld. St. 11 (2012–2013) – personvern – utsikter og utfordringar – vedlegges protokollen.

Oslo, i kommunal- og forvaltningskomiteen, den 29. april 2013

Aksel Hagen
leder

Michael Tetzschner
ordfører