DET KONGELEGE FORNYINGS-,
ADMINISTRASJONS- OG KYRKJEDEPARTEMENTET

Meld. St. 11

(2012–2013)

Melding til Stortinget

Personvern – utsikter og utfordringar

Innhald

DET KONGELEGE FORNYINGS-,
ADMINISTRASJONS- OG KYRKJEDEPARTEMENTET

Meld. St. 11

(2012–2013)

Melding til Stortinget

Personvern – utsikter og utfordringar

Tilråding frå Fornyings-, administrasjons- og kyrkjedepartementet 14. desember 2012, godkjend i statsråd same dagen.
(Regjeringa Stoltenberg II)

1 Samandrag

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.

Utgangspunktet for denne meldinga er rapporten *Individ og integritet – personvern i det digitale samfunnet* utarbeidd av Personvernkommisjonen og innteken i NOU 2009: 1. Regjeringa tek likevel ikkje sikte på å omtale alle framlegga frå Personvernkommisjonen i meldinga. Meldinga gjer greie for korleis ein kan bruke handlingsrommet i personvernregelverket til beste både for samfunnet, for innbyggjarane og for dei som behandlar personopplysningar. Dette vil leggje grunnlag for betre personvern, slik Personvernkommisjonen etterlyser.

Internasjonalt personvernregelverk, med konsekvensar for den norske personvernreguleringa, gjennomgår for tida store revisjonar. Regjeringa vil vente på desse regelendringane før ho vurderer endringar i den norske personopplysningslova. I denne meldinga blir det derfor ikkje gjort framlegg om endringar i gjeldande personopplysningslov. Meldinga gir sektorovergripande tilrådingar innanfor gjeldande personvernregelverk.

Det er viktig at Noreg følgjer den internasjonale utviklinga på personvernområdet og tek aktiv del i arbeidet der utviklings- og regelverksarbeidet skjer. Regjeringa vil arbeide for norsk deltaking i eit eventuelt nytt europeisk datatilsyn og deltaking i avgjerdsprosessane i EU-kommisjonen der dette er aktuelt. Dette blir omtala i *kapittel 3*.

Omsynet til personvernet må ofte vektast mot andre viktige samfunnsomsyn og interesser. Slik vekting kan vere vanskeleg og krev grundige vurderingar frå område til område og frå sak til sak. Vurderingane er viktige for at ein skal kunne ta omsyn til dei ulike interessene på best mogleg måte. I *kapittel 4* blir det gjort greie for vurderingar på nokre sentrale område.

Tilrettelegging for gjenbruk av offentlege data er ein viktig del av politikken til regjeringa, og ein skal i så stor grad som råd leggje til rette for gjen-

bruk av offentlege informasjonsressursar. Ulike døme på gjenbruk og moglegheiter og utfordringar knytte til gjenbruken blir drøfta i *kapittel 5*.

Behandling av personopplysningar skal alltid ha eit behandlingsgrunnlag i samsvar med personopplysningslova. Dette blir omhandla i *kapittel 6*. Eit behandlingsgrunnlag kan vere ein lovheimel, eit samtykke frå den registrerte eller at behandlinga er nødvendig for eit nærmare oppgitt føremål. Forvaltninga si innsamling og bruk av personopplysningar er i hovudsak fastsett i lov eller er nødvendig for å utøve offentleg styresmakt. Informasjon om og samtykke til behandling av personopplysningar er likevel viktige personvernprinsipp. Samtykke bør òg i framtida vere det føretrekte behandlingsgrunnlaget i samanhengar der dei registrere reelt kan velje om dei vil vere registrerte. Å gi dei registrerte ein rett til å reservere seg mot behandling av personopplysningar kan vere ei god personvernløysing der personopplysningsbehandlinga er lovleg, men likevel ikkje påkravd.

Somme gonger manglar både mindreårige og vaksne samtykkekompetanse. Dette reiser særlege utfordringar. I mange samanhengar samtykkjer vaksne i behandling av personopplysningar på vegner av barn. Då skal dei alltid ta omsyn til det som er best for barnet. Dei bør òg leggje vekt på kva barnet sjølv meiner, også der barnet ikkje har sjølvstendig samtykkekompetanse.

I kapittel 7 blir det gjort greie for ulike personvernrettar og -plikter og korleis ein best kan oppfylle dei. Det er eit klårt mål at folk skal ha råderett over eigne personopplysningar og vere i stand til å ta vare på sitt eige personvern. Dei registrerte skal ha informasjon om kva opplysningar som blir nytta om dei til ulike føremål, og kjenne personvernrettane sine. Både offentlege verksemder og private behandlingsansvarlege har ansvar for at dei registrerte får den nødvendige informasjonen på ein enkel og lettfatteleg måte.

I arbeidet regjeringa gjer med digitalisering av offentleg sektor er det mogleg å finne fram til elektroniske løysingar som sikrar omsynet både til digitalisering og personvern. Når ein implementerer slike løysingar, må ein sjå til at systemet tek vare på informasjonstryggleiken på ein god måte.

Dataminimalitet er eit viktig prinsipp i personvernsamanheng. Dataminimalitet går ut på å avgrense mengda av personopplysningar så mykje som mogleg ut frå føremålet med behandlinga. Når ein greier ut ulike tiltak som har eller kan ha personvernkonsekvensar, skal prinsippet om dataminimalitet ha stor vekt. Det er eit mål å leggje til rette for bruk av sporfrie alternativ der det ikkje er nødvendig å identifisere seg.

Kapittel 8 handlar om personvern og sosiale medium. Bruken av sosiale medium har vakse enormt dei seinare åra og kan føre til store personvernutfordringar for brukarane.

Det er særleg barn og unge som er utsette for krenkingar på nett. Det er derfor viktig å vidareføre og styrkje førebyggjande arbeid gjennom informasjon og haldningsskapande verksemd overfor desse aldersgruppene.

Teknologien kan utfordre personvernet. Samstundes kan ein òg bruke teknologi til å styrkje personvernet. I *kapittel 9* blir bruk av ulike teknologiar som både kan utfordre og støtte opp under etterleving av personvernregelverket drøfta.

Med innebygd personvern meiner ein som oftast bruk av teknologi for å ta vare på personvernet. Ein bør til dømes setje førehandsdefinerte standardinnstillingar i teknologisk utstyr, system og program til det mest personvernvenlege nivået. Det bør vere eit mål å gjennomføre innebygd personvern i alle sektorar.

Lagring av data i nettskya blir stadig vanlegare. Det er både rimeleg og praktisk for mange. Rettleiingar om korleis ein kan gjere nettskyavtalar tilpassa ulike sektorar, kan vere eit godt hjelpemiddel for å ta vare på ulike omsyn ved bruk av nettskya.

Eit viktig element i alt arbeid med informasjonstryggleik er styring av tilgangen til informasjon. Logging av tilgang kan vere eit middel for å kontrollere om tilgangsstyringa verkar. Regjeringa har vedteke å setje ned ei arbeidsgruppe som skal greie ut behovet for klientbasert logging i større offentlege og private register. Gruppa vil undersøkje korleis logging blir praktisert i aktuelle sektorar og register, korleis innsynsretten blir praktisert, og korleis ein bør praktisere logging og innsyn i loggar i dei ulike sektorane i framtida.

Datatilsynet er både tilsynsstyremakt og ombod for personvernet, og blir omtala i *kapittel 10*. Det er viktig at etaten er tydeleg på dei ulike rollene sine og kva for verkemiddel som kan takast i bruk. Den raske teknologiske utviklinga fører til krevjande og veksande oppgåver for Datatilsynet. Dei siste åra har tilsynet arbeidd mykje med strategiar og planar for å kunne møte framtidige utfordringar betre og bruke ressursane sine på ein god måte.

Personvern er eit rettsområde der både utfordringar og løysingar er internasjonale. Deltaking i internasjonalt personvernarbeid er derfor viktig. Datatilsynet prioriterer internasjonalt arbeid og har nyleg utarbeidd ein strategi for det internasjonale engasjementet sitt.

Verksemder som ønskjer å ha særskild merksemd retta mot personvern, kan tilsetje person-

vernombod/personvernrådgivar. Ein personvernrådgivar med klåre oppgåver og ei sterk forankring i leiinga i verksemda kan ha positiv effekt på korleis verksemda tek vare på personvernomsyna. Ordninga kan òg vere ei avlasting for Datatilsynet. I lys av EUs revisjon av personverndirektivet kan det bli aktuelt å sjå på ordninga med personvernombod/personvernrådgivarar og gi ho ei klårare forankring i personvernregelverket.

2 Innleiing

På mange samfunnsområde, og både i privat og offentleg verksemd, er det nødvendig og ønskjeleg å samle inn, bruke og utveksle personopplysningar mellom aktørar både nasjonalt og internasjonalt. 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.

2.1 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 og hadde dette omfattande oppdraget:

- Gi ein heilskapeleg status over utfordringane for personvernet. I samband med dette skal kommisjonen skildre dagens situasjon og utfordringar innan ulike sektorar som den ser som særleg relevante, og sjå hen til internasjonale avtaler og regelverk knytta til personvern.
- Vurdera nærmare korleis personvernet bør takast vare på i møte med motståande omsyn og verdiar.
- Kartleggje og evaluere dei verkemidla som i dag eksisterer for å ta vare på personvernet, herunder sjå på personvernstyresmaktenes praksis og rolle.
- Fremje forslag til nye prinsipp og verkemiddel, samstundes som andre omsyn óg vert tekne vare på. I denne samanheng skal kommisjonen vurdere bruk av personvernfremjande teknologi.
- Sjå på moglege tiltak og verkemiddel for betre etterleving av regelverk som tek vare på personvernet.

Kommisjonen leverte rapporten sin til Fornyings- og administrasjonsdepartementet 13. januar 2009. 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.

Denne meldinga byggjer på mange av funna frå arbeidet Personvernkommisjonen gjorde, og på innspela frå høyringsrunden. Personvern er relevant for svært mange samfunnsfelt, men er sjeldan i seg sjølv målet med eit arbeid. For eksempel er behandling av personopplysningar heilt nødvendig for å kunne yte god helsehjelp, for å kunne drive effektiv kriminalitetsførebygging og for å kunne administrere ulike velferdsordningar, men er likevel ikkje eit mål i seg sjølv. Når ein utviklar og implementerer ny teknologi, eller når ein set i verk ulike tiltak som inneber behandling av

personopplysningar, er personvernvurderingar sjeldan i sentrum. Men personvern er eitt av fleire moment som ein må vurdere og ta omsyn til i eit arbeid. Oftare og oftare ser ein at det ikkje blir teke godt nok vare på personvernet fordi utgreiarane og avgjerdsstakarane, både i offentleg og privat sektor, ikkje har vurdert personvernkonsekvensane grundig nok eller sett i verk tiltak som kan ta vare på personvernomsyna tidleg nok.

I samband med behandlinga av innstilling til Stortinget om gjennomføring av EUs datalagringsdirektiv[1], bad Stortinget om nærmare utgreiing av fleire tema på personvernområdet. Dette gjeld krav til logging, gjennomgang av rutinar for å sikre teieplikta i Arbeids- og velferdsetaten og ordninga med personvernombod. Desse temaa vert omtalte i meldinga.

Meldinga byggjer òg på det som er sagt i Soria Moria-erklæringa om varetaking av personvernomsyn. Om dette heiter det i kapittel 6 i erklæringa:

> «Det må settes klare grenser for hvor langt offentlige myndigheter og andre kan gå i retning av innsyn i, eller kontroll med den enkeltes gjøremål. Retten til likeverdig behandling i rettsapparatet og forvaltningen, og enkeltmenneskets rett til vern om eget privatliv er grunnleggende prinsipper i en rettsstat. Ytringsfriheten skal være reell, både i arbeidsliv og i privatliv. Retten til å være informert er avgjørende for muligheten folk har til å delta i samfunnsdebatten.
>
> Personvernet 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.»

Regjeringa ønskjer å drøfte sektorovergripande mål og tiltak for eit betre personvern. Det er nødvendig med sektorovergripande og langsiktige mål som kan liggje fast i personvernarbeidet. Meldinga skal derfor ikkje på same måten som rapporten frå Personvernkommisjonen drøfte personvern knytt til særlege sektorar og einskildtiltak i desse sektorane. I staden vil regjeringa peike på generelle personvernprinsipp, -mål og -tiltak ein kan tilpasse og bruke på personvernutfordringar same kva samfunnsområde det gjeld. Med ei slik tilnærming vonar regjeringa å leggje grunnlag for ein debatt om varetaking av personvern i samfunnet i dag og presentere nokre tiltak for korleis ein best mogleg kan ivareta gjeldande regelverk.

2.2 Avgrensing mot delar av rapporten frå Personvernkommisjonen

2.2.1 Strukturen i rapporten – korleis regjeringa vurderer einskilde tiltak

Som tidlegare sagt tek regjeringa ikkje sikte på å gå gjennom alle framlegga frå Personvernkommisjonen i denne meldinga. Nedanfor blir det likevel kort gjort greie for korleis regjeringa allereie har følgt opp fleire av framlegga frå Personvernkommisjonen på ulike område, sjå kapittel 2.3. Meldinga skal òg gjere 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 er derfor ikkje eit mål at alle framlegga frå kommisjonen skal omtalast i denne meldinga. Dei ulike framlegga frå Personvernkommisjonen til tiltak som kan betre personvernet på dei konkrete områda, vil derimot vere med i vurderingane når sektorstyremaktene arbeider med ulike tiltak på kvart sitt område, til dømes i arbeidet som er i gang med å revidere lov 9. juni 1989 nr. 32 om pliktavlevering, eller i arbeidet regjeringa gjer med e-helse. 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. 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.

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 denne meldinga. Det blir alltid gjort grundige personvernvurderin-

[1] Inns. 275 L (2010-2011)

gar 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.

2.2.2 Grunnlovsfesting av personvern

Grunnlovsfesting av personvernet kan synleggjere personvernet som menneskerett og kva rom denne retten bør ha i samfunnet vårt. Personvernkommisjonen viser i si utgreiing kapittel 19.1 mellom anna til den ubalansen det er at ytringsfridom som grunnleggjande rett er grunnlovsfesta, medan retten til personvern, som av og til står i motstrid til ytringsfridom, ikkje er det. Samstundes er det slik at dei grunnlovsfesta rettane alltid vil ha stor vekt i tolking og bruk av anna regelverk. Med grunnlag i mellom anna ei utgreiing av Alf Petter Høgberg og Njål Høstmælingen[2] konkluderer Personvernkommisjonen i rapporten sin med at retten til personvern bør grunnlovsfestast i Noreg.

Grunnlovsfesting av menneskerettar er òg vurdert av det stortingsoppnemnde Menneskerettsutvalet[3]. Utvalet leverte rapporten sin 10. januar 2012[4]. I kapittel 30.6.5 skriv utvalet følgjande om grunnlovsfesting av personvern:

> «En grunnlovsfesting av privatlivets fred, personvern og personopplysningsvern vil i første rekke ha den konsekvens at disse prinsippene får en generell forankring i Grunnloven. Det vil synliggjøre at den fragmentariske lovgivning på området og det ulovfestede vern etablert av domstolene, springer ut av en grunntanke om at det finnes en privatsfære som omverdenen ikke har krav på innsyn i, men som tvert i mot har krav på beskyttelse mot slikt innsyn.
>
> Videre vil grunnlovsfesting bidra til å løfte de internasjonale menneskerettighetsprinsipper om «right to privacy» inn i en norsk kontekst. En norsk grunnlovsbestemmelse om privatlivets fred mv. vil kunne speile essensen i både de internasjonale menneskerettighetsbestemmelsene, den ordinære lovgivning og det ulovfestede personvern. Slik vil en grunnlovsbestemmelse på dette området ikke endre dagens rettstilstand, men bidra til å synliggjøre den gjennom en prinsipiell bestemmelse i Grunnloven.»

Vidare skriv utvalet

> «En grunnlovsfesting av privatlivets fred, personvern og personopplysningsvern vil fremheve det rettslige utgangspunkt om ivaretakelse av disse verdiene i norsk rett. Den nærmere vurderingen eller avveiningen av hvor langt en slik grunnlovsbestemmelse strekker seg, vil måtte forstås i lys av og suppleres med det internasjonale konvensjonsvernet og med tidligere ulovfestet rett. Hensikten med en slik grunnlovsbestemmelse vil dermed være å sikre at privatlivets fred, personvern og personopplysningsvern sikres på alle rettsområder i tråd med gjeldende praksis, samtidig som dette synliggjøres på grunnlovs nivå.»

Grunnlovsfesting av retten til personvern endrar ikkje 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. Regjeringa vil derfor ikkje gjere ytterlegare vurderingar av spørsmålet om grunnlovsfesting av personvernet i denne meldinga.

2.3 Tilrådingane frå Personvernkommisjonen – gjennomførte tiltak

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.

---

2 Betenkning om grunnlovsfesting av retten til personvern/privatliv, Alf Petter Høgberg og Njål Høstmælingen, overlevert Personvernkommisjonen den 3. november 2008

3 Dokument 16 (2011–2012) Rapport fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven, avgitt 19. desember 2011

4 http://www.stortinget.no/Global/pdf/Dokumentserien/2011-2012/dok16-201112.pdf

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*. Medieansvarsutvalet (NOU 2011: 12) greidde óg ut behovet for særskilde lovreglar eller tenester som kan tryggje personvernet til einskildpersonar i møte med media. Utvalet gjorde ikkje framlegg om nye lovføresegner, men såg behovet for eit lågterskeltilbod som kan bidra til å løyse usemjer innanfor sosiale medium og andre medium utan ein sentral redaktørfunksjon. Medieansvarsutvalet peikte særleg på informasjons- og hjelpetenesta *slettmeg.no*. Tenesta, som vart etablert som ei direkte følgje av framlegget frå Personvernkommisjonen, vart i oppstarts- og prosjektperioden driven av Datatilsynet med finansiering frå Fornyings-, administrasjons- og kyrkjedepartementet. Frå 1. januar 2012 har tenesta vore driven av NorSIS. Tenesta har hatt stor pågang og har hjelpt mange som har opplevd integritetskrenkingar gjennom spreiing av bilete og andre personopplysningar på nettet. 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. Regjeringa er svært nøgd med at NorSIS driv tenesta vidare.

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 innstramming 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. I dag er skattelistene berre tilgjengelege frå nettsidene til skatteetaten, og innsyn krev innlogging med MinID. Det avgrensar innsynet vesentleg og tek vare på ønsket skattytarane har om diskresjon. Pressa har ikkje lenger rett til å offentleggjere heile skattelister elektronisk.

Personvern i arbeidslivet

Bruken av teknologi i arbeidslivet aukar sterkt. Bruk av teknologi i arbeidet eller som eit kontrolltiltak let i dei fleste tilfelle etter seg spor som seier kva arbeidstakaren har gjort, når det vart gjort, kor lang tid det tok, og ofte òg kvar det vart gjort. Eit av tiltaka Personvernkommisjonen gjer framlegg om for å betre personvernet for dei tilsette, er å regulere tilgangen arbeidsgivaren har til e-posten dei tilsette sender og tek imot. Då kommisjonen kom med framlegget, hadde regjeringa alt i lang tid arbeidd med eit forskriftsframlegg som skulle regulere tilgangen arbeidsgivaren har til e-posten til dei tilsette og til elektronisk lagra dokument på personlege område. 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[5] vart endra 19. juni 2009. Dette inneber at viktige element i framlegget frå Personvernkommisjonen for å betre personvernet i helsesektoren er gjennomførte.

Barn og personvern

Den teknologiske utviklinga gjer at bilete og opplysningar om barn lett kan spreiast på nettet, og det aukar risikoen for misbruk av personopplysningar om barn. Utfordringar kan til dømes kome når skule, barnehage og foreldre/føresette legg ut personopplysningar om barn på internett. Personvernkommisjonen peikte i rapporten sin på at ein særleg treng reglar som kan verne barn mot uønskt publisering av personopplysningar på internett. 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.

---

[5] Lov om helseregistre og behandling av helseopplysninger 18. mai 2001

2.4 Avgrensing mot igangsett arbeid med personvernkonsekvensar

Kvart departement og kvar etat har ansvar for personvernarbeid i sin sektor og skal tryggje personvernomsyn i arbeidet sitt. Det blir til kvar tid arbeidd med tiltak som får personvernkonsekvensar. Denne meldinga tek sikte på å drøfte sektorovergripande personvernutfordringar og gi råd om korleis desse utfordringane generelt kan møtast og handterast. Kvar sektor må ta ansvar for å handtere sektorspesifikke utfordringar, med grunnlag i dei felles løysingane og prinsippa ein kjem fram til. Det er derfor nødvendig å gjere kort greie for personvernrelatert arbeid som er i gang i nokre sektorar, og som ikkje vil bli nærmare omtala i denne meldinga.

2.4.1 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. Kva kontrolltiltak verksemda har høve til å setje i verk overfor dei tilsette, blir regulert av arbeidsmiljølova. Bruken av dei opplysningane som kjem fram som ei følgje av kontrolltiltaket, blir regulert av personopplysningslova. Ny teknologi opnar for nye former for kontroll og overvaking av arbeidstakarane. Dette får konsekvensar for personvernet til dei tilsette, men òg for sjølve arbeidsmiljøet.

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. Arbeidstilsynet kan no gi dei pålegga som er nødvendige for å sikre at reglane om kontroll og overvaking i arbeidsmiljølova blir følgde. Dette har skapt ein meir effektiv sanksjonsmåte og er meir i samsvar med fullmaktene Datatilsynet har etter personopplysningslova.

Det har såleis vore ei utvikling sidan 2005, og rettstilstanden har òg skifta etter at Personvernkommisjonen kom med rapporten sin. 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. Arbeidsgruppa er samansett av representantar for partane i arbeidslivet og for arbeidslivs- og personvernstyremaktene og er framleis i byrjinga på arbeidet. 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. Det er derfor nødvendig at partane og tilsynsstyremaktene saman arbeider vidare med utfordringar knytte til kontroll og overvaking/personvern i arbeidslivet og kjem attende med konklusjonar og personverntiltak i arbeidslivet ved eit seinare høve.

2.4.2 Barne- og likestillingssektoren

Barne-, likestillings- og inkluderingsdepartementet arbeider med reglar om openheit kring løn som eit tiltak for likeløn og mot lønsdiskriminering. Departementet gjer framlegg om nye reglar i diskrimineringslovgivinga om utarbeiding av kjønnsdelt lønsstatistikk på verksemdnivå og om opplysningsplikt ved mistanke om lønsdiskriminering. Dersom opplysningane som blir gitt, avslører løna til einskildpersonar, kan dette kome i strid med interessa arbeidstakaren har i diskresjon. Personvernomsyn er derfor eit tema i regelverksarbeidet, og framlegga er utforma i samsvar med reglane i personopplysningslova og prinsippa som følgjer av denne meldinga. Framlegget er ein del av arbeidet regjeringa gjer med ein lovproposisjon om endringar i diskrimineringslovgivinga som etter planen skal fremjast i 2013.

Gjeldsregistrering

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.

Bakgrunnen for tiltaket er at gjeldsproblem hos private er eit stort og aukande problem. Tal frå

namsstyremaktene viser ein jamn auke i talet på utleggsforretningar dei siste tre åra, og talet på personar under offentleg gjeldsordning har aldri vore høgare enn i 2011. For mange er det for store opptak av usikra forbrukskreditt (forbrukslån og kredittkort) som er hovudårsaka eller ei medverkande årsak til gjeldsproblema. Finansføretak har teieplikt om låneavtaler med eigne kundar, og når dei vurderer lånesøknader, har føretaka derfor ikkje høve til å kontrollere opplysningane lånesøkjaren gir om eksisterande gjeldsskyldnader til andre føretak. Regjeringa ønskjer å sjå på om det er mogleg å endre teieplikta bankane og finansføretaka imellom, slik at informasjon om forbrukskredittane til lånesøkjaren kan vere tilgjengeleg for kredittytaren ved vurdering av nye lånesøknader.

Etablering av eit system for registrering og bruk av opplysningar om usikra forbrukskreditt gir likevel utfordringar når det gjeld personvernet. Desse utfordringane er særleg knytte til kva opplysningar som skal kunne registrerast, kven som skal kunne få tilgang, og korleis ein kan sikre god datakvalitet, medrekna kor ofte opplysningane blir oppdaterte. I arbeidet som er i gang, blir det vurdert ulike tiltak for å sikre tilfredsstillande varetaking av sentrale personvernomsyn i samband med gjeldsregistrering.

2.4.3 Finanssektoren

Personvern er eit av fleire viktige omsyn i arbeidet med regulering av finanssektoren. Bank- og forsikringsverksemd inneber ofte behandling av opplysningar som kan ha personvernkonsekvensar i ulike samanhengar.

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.

2.4.4 Helse- og omsorgssektoren

Det blir stadig fleire eldre i befolkninga, og talet på personar med kroniske sjukdomar aukar. Helse- og omsorgssektoren står derfor overfor store utfordringar, mellom anna i form av aukande kompleksitet i sjukdomsbiletet, talet på pasientar og innbyggjaranes forventningar til tenesta. For å sikre tilliten og berekrafta til den offentlege helse- og omsorgstenesta må ein ta i bruk meir moderne og effektive hjelpemiddel for informasjon og kommunikasjon. Dette skal gjerast på ein måte som tek betre vare på samspelet mellom forventninga om godt integritetsvern og god pasienttryggleik. Ein må sikre heilskaplege pasientgangar, og det må leggjast til rette for samhandling mellom helsearbeidarar, som blir alt meir spesialiserte. Vidare er det ein del av utfordringsbiletet at det totalt blir utført i overkant av 220 000 årsverk i helse- og omsorgssektoren, og at det årleg er ca. 4 millionar sjukehusopphald og ca. 4,3 millionar polikliniske konsultasjonar.

I helse- og omsorgssektoren er arbeid med personvern, til liks med betring av tenestetilbodet, kontinuerlege prosessar. Parallelt med denne meldinga 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 her.

Samhandlingsreforma og fokuset på føresetnaden om ein heilskapleg pasientgang demokratiserer helsetenesta ved å involvere brukarar og pasientar i større grad enn i dag. Pasienten blir sett i stand til å vere ein aktiv deltakar i varetakinga av si eiga helse. 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. Utviklinga innanfor sporings- og varslingsteknologien, for eksempel bruk av GPS, har opna for nye måtar å skape tryggleik på ved å gjere det lettare å finne att personar med svak orienteringsevne og sikre at dei kan ferdast friare enn dei elles hadde kunna gjere. Dette kan gi meir fysisk aktivitet og eit sjølvstendig liv for kvar einskild. Regjeringa arbeider med å leggje til rette eit tilfredsstillande rettsleg grunnlag for bruk av denne typen teknologi. Forslag til endringar av korleis ein kan bruke varslings- og lokaliseringsteknologi, er allereie sende på høyring.

Respekt for integriteten til pasienten er ei grunnleggjande etisk norm ved all helsehjelp. Pasientane skal mellom anna vernast mot spreiing av opplysningar om personlege tilhøve og helsa si. Helsearbeidarar er derfor pålagde teieplikt. Teieplikta skal òg tryggje tilliten mellom helsetenesta

og brukarane og medverke til open kontakt mellom pasientar og helsepersonell. Det går jamleg føre seg opplærings- og haldningsskapande tiltak som skal sikre at teieplikta blir ivareteken. Det er mellom anna utarbeidd eit rundskriv som gir helsepersonell ei lett tilgjengeleg rettleiing om teieplikta dei har i den direkte, munnlege kommunikasjonen med pasientar. 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.

2.4.5 Justissektoren

Delrevisjon av personopplysningslova

I forarbeida til personopplysningslova vart det uttrykt behov for etterkontroll av lova for å undersøkje om reglane verkar slik dei var meinte. 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 teknologiske utviklinga gjer at bilete av og opplysningar om barn lett kan spreiast på nettet, noko som aukar risikoen for misbruk av personopplysningane. 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. Det har vore ein stor auke i talet på kamera som er monterte i det offentlege rommet, og kjensla av å vere overvaka kan vere sterk hos mange. Samstundes kan kameraovervaking vere med og gi auka tryggleik og oppklaring av kriminalitet. Med dei nye reglane er definisjonen av kameraovervaking 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. Lovendringa gir Datatilsynet kompetanse til å gjere unntak frå konsesjonsplikta etter skjøn for behandling av personopplysningar som ikkje representerer nokon reell fare for personvernet. Slik blir saksmengda hos tilsynsstyremakta avgrensa, samstundes som fordelane ved konsesjonsordninga blir førte vidare.

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. Framlegget fekk brei tilslutning under høyringa og er dessutan i tråd med utgreiinga frå Medieansvarsutvalet[6]. Bakgrunnen for endringa var at tilsynsstyremakta har late vere å gripe inn mot nettytringar av til dels sjikanerande karakter med den grunngivinga at dei har vore opinionsdannande ytringar.

I EU går det for tida føre seg eit arbeid med å vedta nye reglar om behandling av personopplysningar. Reglane skal avløyse direktiv 95/46/EF. Med framlegga i Prop. 47 L (2011–2012) tok regjeringa sikte på å møte behovet for oppdatering av visse delar av personopplysningslova i påvente av revisjonsarbeidet i EU. Når dei nye EU-reglane 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. Denne 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. Regelverk som blir utvikla på desse områda innan Schengen-samarbeidet, blir implementerte i norsk rett. Biometriske

[6] Jf. NOU 2011: 12 Ytringsfrihet og ansvar i en ny mediehverdag.

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. I VIS blir saksopplysningar om søkjaren, i tillegg til fingeravtrykk av personar over tolv år, lagra i inntil fem år. Schengen-medlemslanda kan, innanfor nærmare gitte rammer, få tilgang til informasjonen i samband med behandlinga av visumsøknader, grensekontroll og identifisering. Vidare kan Europol og politistyremakter med ansvar for å førebyggje, granske eller oppklare terrorhandlingar eller annan alvorleg kriminalitet, få tilgang på nærmare fastsette vilkår.

Ved utviklinga av regelverk innan Schengensamarbeidet legg EU-kommisjonen og Schengen-medlemslanda 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. Kriminalomsorga treng informasjon frå politiet for å sikre den generelle tryggleiken i fengsla. Vidare treng kriminalomsorga tilstrekkeleg informasjon frå politiet, slik at ho kan setje inn nødvendige tryggingstiltak rundt kvar einskild innsett for å førebyggje eller hindre ny kriminalitet. Politiet treng informasjon om den innsette for å kunne førebyggje eller hindre alvorleg kriminalitet.

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 beredskapsdepartementet i 2010 ned eit utval. INFOFLYT-utvalet leverte rapporten sin til departementet 22. mai 2012. I rapporten er det mellom anna gjort framlegg om eit klårare heimelsgrunnlag for INFOFLYT, medrekna reglar om utlevering av opplysningar frå kriminalomsorga til politiet. 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). Mellom anna vart risikovurdering, avviksrapportering og -handtering gjennomgått. Alle tilsette har i samband med dette fått opplæring i krava personopplysningslova set til informasjonstryggleik.

2.4.6 Utdanningssektoren

Sentralt elevregister

Grunnopplæringa og utdanningsstyremaktene, medrekna Kunnskapsdepartementet og Utdanningsdirektoratet, treng eit godt kunnskapsgrunnlag for å gjere norsk skule betre. Utdanningsdirektoratet har mellom anna ansvar for utviklingsprosjekt, forsking og statistikk om grunnskulen og den vidaregåande opplæringa. På nettsidene til Utdanningsdirektoratet blir det framlagt resultat og analysar, og det blir òg jamleg sendt kunnskapsgrunnlag til Kunnskapsdepartementet. Utdanningsdirektoratet behandlar i dag nokre personopplysningar på individnivå frå vidaregåande opplæring. Desse personopplysningane blir

hovudsakleg henta frå inntakssystemet til vidaregåande opplæring (Vigo) hos fylkeskommunane.

I oktober 2008 sende regjeringa eit framlegg om å etablere eit sentralt individbasert og pseudonymt elevregister i skulesektoren på høyring. Framlegget innebar at Utdanningsdirektoratet skulle halde fram med å behandle personopplysningar frå vidaregåande opplæring, og at behandlinga òg skulle femne om visse personopplysningar frå grunnskulen. 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. Berre ved slik lagring kan datagrunnlaget opne for analysar, statistikk og forsking og medverke til at staten kan sikre retten til grunnopplæring. Det vart derfor gjort framlegg om å klårgjere gjeldande rett.

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.

2.4.7 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.

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 strafferettslege redaktøransvaret, men i ei meir medieuavhengig form. Det nærmare innhaldet i ei særskild regulering av ansvarssystemet for media blir nærmare utgreidd av Kulturdepartementet i samråd med dei aktuelle departementa.

2.4.8 Samferdselsektoren

Grovt sett er det 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. Utviklinga går mot ei heilautomatisering av bompengeanlegg i Noreg. Passeringsdata blir lagra, og det utfordrar retten til anonym ferdsel. Det er eit klårt politisk ønske å kunne tilby ei fullt anonym bompengeløysing, særleg for privatbilistar. 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. Kravet blir i dag etterlevd av bompengeselskapa. Det er viktig å finne ei permanent løysing på desse utfordringane relativt raskt.

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 trafikktrygg-

leiken. Enkelt sagt får nye køyretøy installert ein telefon som ringjer nødnummeret dersom bilen er involvert i ei ulukke. Innleiingsvis i samtala blir det oversendt tekniske data om køyretøyet og kvar det står. I utforminga av eCall i EU, og i standardiseringsarbeidet der, har personvernspørsmål vore sentrale. *The Article 29 Data Protection Working Party (sjå nærmare omtale i kapittel 3.2)* og norske representantar er involverte i diskusjonane på EU-nivå. 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 som er knytt opp mot ein nasjonal standard, og som Vegdirektoratet forvaltar (jf. omtale i kapittel 9.4.2)

2.4.9 Teieplikt og opplysningsplikt i førebyggjande verksemd

Teieplikt og personvern heng nøye i hop. Gode reglar om teieplikt og rett praktisering av reglane kan vere ein føresetnad for god ivaretaking av personvernet til dei registrerte. Samstundes er det nødvendig å leggje til rette for utveksling av informasjon underlagd teieplikt innanfor trygge rammer når dette er nødvendig for å ta vare på interessene til både einskildmenneske og samfunnet.

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. Arbeidsgruppa er forankra i førebyggingsstrategien til regjeringa *(Regjeringens strategi for forebygging: Fellesskap – trygghet – utjevning (Departementene 2009))* og er vidare omtala i den kriminalitetsførebyggjande handlingsplanen til regjeringa (*Gode krefter – Kriminalitetsforebyggende handlingsplan (Justis- og politidepartementet, 2009)*). Målet er å gå gjennom eksisterande regelverk for teieplikt og informasjonsutveksling i dei relevante fagmiljøa (helse- og omsorgssektoren, barnevernet, utdanningssektoren, kriminalomsorga og politiet) for å avdekkje eventuelle svake punkt og vurdere om det trengst lovendringar. Arbeidet tek sikte på å følgje opp eit vidfemnande kartleggingsprosjekt om same emnet, som Helse- og omsorgsdepartementet har ansvaret for. Personvernomsyn vil bli vurderte i dette arbeidet.

2.4.10 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. Dette er i tråd med FADs koordineringsansvar for den nasjonale IKT-politikken. Meldinga vil ha verdiskaping basert på bruk av IKT som overordna mål og femne om tema som breiband, digital kompetanse og digitalisering i næringsliv og offentleg sektor. Ho vil òg drøfte emne som avansert IKT-kompetanse og sårbarheit. 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. Å behandle personopplysningar er ein nødvendig føresetnad for forvaltninga, både som utøvar av offentleg myndigheit og som tilbydar av tenester. Digitalisering og personvern kan gå hand i hand om ein bruker dei mogleghetene teknologien gir til å ta vare på personvernet. Mellom anna kan gode digitale løysingar gi grunnlag for store innsparingar i offentleg forvaltning, samstundes som det kan gi lettare tilgang til eigne personopplysningar for innbyggjarane.

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. Programmet kviler på ein føresetnad om at ei digital forvaltning gir betre tenester, og at digitalisering av forvaltninga gjer sitt til å frigjere ressursar til andre område. Digitalisering skal både gi innbyggjarane og næringslivet eit betre og raskare møte med offentleg sektor og betre ressursbruken i offentleg sektor.

Digitalisering av offentleg forvaltning skal medverke til at det blir enklare å bruke offentlege tenester. Digitalisering opnar òg for at tenester frå ulike verksemder kan koplast saman i éi og same nettenesta, slik at ein kan få utført tenester frå fleire offentlege etatar i eitt og same ærendet. Bruk av personopplysningar på tvers av etatsgren-

ser, 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.

3 Personvern i eit internasjonalt perspektiv

3.1 Innleiing

Dei internasjonale rettslege instrumenta og det internasjonale samarbeidet på personvernområdet blir stadig viktigare. Enorme mengder personopplysningar kryssar landegrensene kvar einaste dag. Nokre opplysningar overfører dei registrerte sjølve, både medvite og umedvite, men mange opplysningar blir òg overførte av dei behandlingsansvarlege. 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. Nedanfor blir det gjort greie for nokre viktige utviklingstrekk på det internasjonale området etter at Personvernkommisjonen avslutta arbeidet sitt.

3.2 EUs personverndirektiv og europeisk personvernsamarbeid

Arbeidet med EUs direktiv 95/46/EF (heretter omtala som personverndirektivet) vart påbyrja alt på slutten av 1980-talet. Etter vidfemnande ordskifte og ikkje reint få endringsframlegg vart direktivet vedteke i 1995. Personverndirektivet er EØS-relevant og bindande for Noreg.

3.2.1 EU-direktiv som er viktige for norsk personvernregulering

Personverndirektivet er i all hovudsak gjennomført i norsk rett gjennom personopplysningslova frå 2000. 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. Sjølv om personverndirektivet er bindande for Noreg, er det derfor eit stort nasjonalt handlingsrom når nasjonale personvernreglar blir utforma.

Siktemålet med direktivet er å leggje til rette for einsarta ivaretaking av personvernet til innbyggjarane i heile EU/EØS-området i tillegg til å leggje til rette for fri flyt av personopplysningar i den indre marknaden. Personverndirektivet er eit minimumsdirektiv. Dette betyr at einskildstatane kan fastsetje høgare standard for personvern enn det minimumet som følgjer av direktivet. 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. 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.

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. Direktivet inneheld i dag ikkje føresegner om denne typen behandling av personopplysningar, og det er derfor lagt til grunn at ein står fritt til å vedta nasjonale reglar på dette området i den grad dei ikkje strir mot andre EØS-reglar. 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. Desse reglane blir gjeldande for Noreg dersom dei, som det er framlegg om, blir vedtekne som forordning og forordninga òg blir gjord EØS-relevant. 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.

I tillegg til det generelle personverndirektivet i EU er det vedteke direktiv med personvernrelevans på området for elektronisk kommunikasjon. Direktiv 2002/58/EF (kommunikasjonsverndirektivet) inneheld personvernføresegner som gjeld generelt for elektronisk kommunikasjon. Direktivet regulerer mellom anna trygging av kommunikasjon, lagring og vidarebruk av trafikk- og kommunikasjonsdata, spesifisert rekning og abonnentlister (nummeropplysningstenester/-katalogar). 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.

3.2.2 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.

Artikkel 29-gruppa har organisert ei rad undergrupper som arbeider med ulike emne, og i desse undergruppene er EØS-landa med på tilnærma lik line med EUs medlemsstatar. Datatilsynet vurderer desse gruppene som viktige arenaer for å halde seg oppdatert om utviklinga i EU og gir innspel til ulike fråsegner som Artikkel 29-gruppa kjem med. Dette er fråsegner som har mykje å seie for tolking og bruk av personverndirektivet, og som såleis er viktige for rettsutviklinga i EU/EØS-området.

I tillegg til Artikkel 29-gruppa med undergrupper har Datatilsynet dei siste åra prioritert å vere med i fleire arbeidsgrupper saman med dei europeiske datatilsynsstyremaktene, utan at desse formelt er organiserte gjennom eller forankra i EU. Desse gruppene er viktige arenaer for samarbeid og informasjonsinnhenting og blir kort presenterte nedanfor.

The Schengen Joint Supervisory Authority (JSA)

Noreg er fullverdig medlem av dette uavhengige kontrollorganet som er samansett av medlemer frå datatilsynsstyremakter i statar tilknytte Schengenavtala. Representantar frå Datatilsynet er med på møta og har òg vore med på inspeksjonar av korleis andre land handterer pliktene etter Schengenavtala.

Working Party Police and Justice (WPPJ)

Denne arbeidsgruppa 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. Inntil Lisboa-traktaten vart vedteken, var dette området halde utanfor verkeområdet til personverndirektivet. No gjeld derimot dei generelle personvernreglane i EU på dette området òg. Datatilsynet sit i arbeidsgruppa og kan melde inn både generelle problemstillingar og einskildsaker.

Berlin-gruppa

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. Deltaking i gruppa er med og gir Datatilsynet tidleg kunnskap om ulike problemstillingar. Dessutan påverkar gruppa prosessar i EU, og det gir Datatilsynet indirekte påverknad på desse prosessane. Datatilsynet meiner gruppa er eit viktig forum for å drøfte aktuelle personvernutfordringar relaterte til elektronisk kommunikasjon.

Internasjonalt saksbehandlarmøte

Dette 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. Møtet er òg ein god arena for utvikling av kontaktnett, og det er viktig med tanke på handtering av internasjonale saker. Av emna som har vore drøfta på det internasjonale saksbehandlarmøtet dei seinare åra, kan nemnast overføring av personopplysningar til utlandet og problematikk knytt til samarbeid mellom tilsynsstyremaktene i dei ulike landa.

Nordisk møte

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 Nordisk møte. Her møtest leiarane for dei nordiske datatilsynsstyremaktene ein gong i året for å utveksle røynsler frå eiga verksemd. Dei nordiske landa har mange felles drag i personvernreguleringa, og det nordiske møtet er eit viktig samlingspunkt for å finne felles posisjonar som kan dragast inn i det internasjonale arbeidet. Det er òg verdfullt å sjå korleis likearta spørsmål blir løyste i grannelanda våre.

Som oversikta viser, er det etablert ei rekkje samarbeidsforum i Europa som er nyttige arenaer for Datatilsynet både når det gjeld informasjonsinnhenting og utveksling av erfaringar. Det internasjonale samarbeidet blir stadig viktigare for handtering av ulike problemstillingar som landa har felles interesse i å freiste å løyse på så einsarta måtar som råd. Dess meir samla personvernstyremaktene står overfor næringsliv og industri, dess større gjennomslagskraft får dei i personvernspørsmål. Dess meir einsarta personvernpraksis det er i dei europeiske landa, dess lettare blir det òg for næringslivet og dei behandlingsansvarlege å etterleve reglane. Regjeringa meiner derfor det er både bra og viktig at Datatilsynet prioriterer det internasjonale samarbeidet høgt, og at tilsynet bør halde fram med å ta del i det internasjonale samarbeidet så langt dette let seg gjere.

3.2.3 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. Særleg gjeld dette den teknologiske utviklinga, først og fremst med framveksten av internett. Då personverndirektivet vart vedteke, var utviklinga og bruken av internett berre i byrjinga, og ingen spådde det enorme omfanget dette kommunikasjonssystemet skulle få på alle samfunnsområde. Men òg på andre felt har den teknologiske utviklinga, og utviklinga i viljen til å nytte teknologi, vore stor. Mellom anna gjeld dette i helsesektoren, innan samferdsel og i ekomsektoren. Dei fleste daglege gjeremål let etter seg spor som fortel noko om kvar ein person var, når han var der, og i mange tilfelle kva han gjorde.

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. Denne styremakta får då ein slags koordinerande funksjon. 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. Iveren innbyggjarane har synt etter å leggje personopplysningar på nett har gjort det tydeleg at ein treng denne typen slettereglar. Ein rett til å ta med seg personopplysningar frå eitt sosialt nettverk til eit anna er òg eitt av fram-

legga 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 vert 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. Regelutkastet legg stor vekt på rettar og plikter, samstundes som det fokuserer på etablering av sterke og uavhengige personvernstyremakter i dei europeiske landa. 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 straffbare 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. Det er derfor uklårt korleis det endelege regelverket kjem til å sjå ut, like eins når det blir ferdig. 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 denne meldinga.

3.3 OECDs retningsliner om personvern

3.3.1 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. Særs mykje av den internasjonale personopplysningsflyten går mellom Europa og USA/Asia (ofte omtala som APEC-landa, det vil seie land som er medlemer av Asia-Pacific Economic Cooperation). APEC-landa har ei noko anna tilnærming til personvernspørsmål enn den europeiske tradisjonen. I amerikansk rett er det til dømes ein svært nær samanheng mellom personvernspørsmål og forbrukarspørsmål, og personvernrettar er nært knytte til den einskilde som forbrukar. 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. Hovudårsaka til dette er at pliktene i retningslinene i liten grad går ut over pliktene Noreg har gjennom EØS-samarbeidet og EUs personverndirektiv.

3.3.2 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. Samstundes er det sentralt i regelverket at det skal leggje til rette for økonomisk vekst og utvikling ved å minske hindringar for flyt av personopplysningar over landegrensene – eit mål som òg ligg til grunn for EUs personvernregulering. Likevel er det i OECD-samanheng den seinare tida òg retta meir merksemd mot personvern som ein sjølvstendig verdi. Dette kan ein sjå som eit utslag av at flyten av personopplysningar over landegrensene er enorm, og at sjølv om ein ikkje skal hindre denne flyten, er det viktig og nødvendig å leggje til rette for eit godt personvern. Tilliten innbyggjarane har til IKT-system og informasjonsflyt, både nasjonalt og over landegrensene, har mykje å seie for i kva grad dei er villige til å ta systema i bruk. Bruk av ulike IKT-system, ikkje minst for handel, har på si side mykje å seie for den økonomiske utviklinga. Ivaretaking av personvernomsyn, kanskje særleg i den forstand at personopplysningar ikkje skal kome uvedkomande i hende, er derfor viktig ut frå OECDs perspektiv om økonomisk vekst og utvikling. Det er viktig å sjå samspelet mellom økonomisk vekst, trygge IKT-system og personvern. Dette er kome mykje meir i fokus dei seinare åra, mellom anna som følgje av at utviklinga av nettbaserte tenester har skote i vêret.

I 2010 vart det, i høve 30-årsjubileet for OECDs personvernretningsliner, sett i gang eit arbeid med sikte på å revidere retningslinene. I dette arbeidet er OECD oppteken av å modernisere regelverket og i større grad etablere system som kan handtere dei store grenseoverskridande utfordringane ei auka globalisering fører med seg. Revisjonsarbeidet ber i seg mange av dei same prinsippa som ligg til grunn for EUs revisjon av personverndirektivet. 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). Slik Datatilsynet erfarer at internasjonalt personvernarbeid gir nyttig informasjon om korleis andre land handterer personvernutfordringar, erfarer regjeringa at deltaking i OECD-arbeidet òg er til stor nytte.

3.4 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. Komiteen skal kome med framlegg til betringar og endringar i konvensjonen og kan bli beden om å gi fråsegner om endringar eller bruk av konvensjonen. Komiteen har fått namnet *The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (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. I første rekkje er prosessen påbyrja i arbeidsgruppa T-PD. Ein revidert konvensjon kjem i siste instans til å bli vedteken i ministerrådet. Noreg skal vere aktivt med i alle stega i prosessen. Eit viktig omsyn er å tryggje samsvar mellom personvernregelverket som er under utarbeiding i EU, og Europarådskonvensjonen.

3.5 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 – det følgjer av EUs personverndirektiv at slike opplysningar skal kunne flyttast fritt innanfor dette området. 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[1]. 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*.

Standardkontraktane er gitt i form av kommisjonsavgjerder og er ein del av EØS-avtala. Partane i avtala er dataeksportøren og dataimportøren. Det finst ulike variantar av kontraktane, og kva for ein som er den rette å bruke i kvart einskilt tilfelle, er avhengig av den rolla dataimportøren har. Dersom importøren skal vere databehandlar for dataeksportøren, må dei inngå ei avtale om overføring frå ein behandlingsansvarleg til ein databehandlar. Skal importøren behandle opplysningane for eigne føremål, og såleis er å rekne som behandlingsansvarleg for opplysningane som blir overførte, vel dei den kontrakten som er fastsett for overføring til behandlingsansvarlege.

Ved inngåing av standardkontraktane tek partane på seg ulike skyldnader med tanke på å garantere rettane til dei registrerte etter at personopplysningane er overførte. Kontraktane tek opp i seg dei sentrale prinsippa og skyldnadene frå personverndirektivet, samstundes som det finst eigne klausular som plasserer erstatningsansvar, definerer lovval og pålegg partane å rette seg etter avgjerder frå domstolar eller personvernstyremakter i eksportlandet. Overføringar baserte på desse kontraktane skal alltid godkjennast av Datatilsynet på førehand.

Standardkontraktane høver godt for enkelståande overføringar frå eitt selskap til eit anna. I store multinasjonale konsern kan ein likevel trenge hyppige overføringar på kryss og tvers i organisasjonen. Dette kan skape store utfordringar for den som skal halde oversikt over den globale dataflyten, og kva kontraktar som må skrivast mellom dei ulike selskapa i konsernet. I slike tilfelle kan *Binding Corporate Rules* (BCR) vere ei tenlegare løysing.

Ein BCR gir bindande personvernreglar for ein organisasjon og skal mellom anna innehalde eit sett med personvernprinsipp og omtale av prosedyrar som skal tryggje etterleving i praksis. Dessutan må BCR-en vere bindande, både internt i organisasjonen og eksternt overfor rettshavarane.

Føremonene med bruk av BCR er mellom anna at personopplysningar kan flyte fritt innanfor konsernet så snart BCR-en er godkjend, same kvar i verda dataimportøren måtte vere. Det er ikkje nødvendig å kontraktsregulere kvar einaste overføring, og BCR-en sikrar einsarta praksis for behandling av personopplysningane i heile konsernet.

Artikkel 29-gruppa har vedteke eigne prosedyrar for arbeid med BCR, sjå WP 107[2]. Det er søkjaren sjølv som gjer framlegg om kva tilsynsstyremakt som skal leie arbeidet med å godkjenne ein BCR, men det er tilsynsstyremaktene sjølve som avgjer kva styremakt som bør ha ansvaret i kvar einskild sak. Datatilsynet er dei siste åra utpeikt som «lead authority» – eller leiande styremakt – i to saker som gjeld vurdering og godkjenning av *Binding Corporate Rules*. Dette inneber at det er Datatilsynet som skal vurdere og eventuelt til slutt godkjenne dei interne retningslinene for behandling av personopplysningar for to store norske konsern med internasjonal verksemd. Godkjenninga blir i så fall gitt på vegner av alle dei europeiske landa som tek del i samarbeidet, som blir omtala som «the mutual recognition procedure». I dag er dette eit samarbeid mellom 20 land, blant

[1] Sjå arbeidsdokument WP 114 om ei einsarta tolking av artikkel 26 første leddet i direktiv 95/46/EF, http://ec.europa.eu/justice/policies/privacy

[2] Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules", vedteke 14. april 2005.

dei Storbritannia, Frankrike, Tyskland, Irland og dei tre EFTA-landa Island, Liechtenstein og Noreg.

Vurdering og godkjenning av BCR er ei oppgåve som krev store ressursar hos den tilsynsstyremakta som blir utpeikt som leiande styremakt. Dette er ein konsekvens av at BCR-ane ofte har mange hundre sider med kontraktsvilkår, retningsliner for informasjonstryggleik, opplæringsrutinar og så bortetter. Desse skal analyserast og jamførast med det gjeldande personvernregelverket, altså personopplysningslova og direktiv 95/46/EF. Den leiande styremakta er ansvarleg for å sjå til at rettane til dei registrerte blir ivaretekne på tilfredsstillande vis etter at opplysningane er eksporterte ut av Europa.

Det er grunn til å tru at bruken av BCR blir meir utbreidd i framtida. Dette får i så fall konsekvensar for Datatilsynet òg. Grunnen er at ordninga, som i dag berre er lausleg forankra i personvernlovgivinga, etter kvart blir meir kjend og utbreidd. Dessutan er det framlegg om at ordninga no skal konkretiserast og kodifiserast i framlegget frå EU-kommisjonen til personvernforordning, etter at Artikkel 29-gruppa i mange år har oppmoda europeiske verksemder til å nytte denne løysinga for overføring av personopplysningar til land utanfor EØS-området.

3.6 Samandrag og tilrådingar

Auka globalisering, meir bruk av internett og veksande samhandling over landegrensene fører med seg enorm flyt av personopplysningar. Personvern er derfor eit internasjonalt fagområde. Ein må drøfte og løyse utfordringar internasjonalt. Noreg vil arbeide for deltaking i eit eventuelt nytt europeisk datatilsyn og deltaking i avgjerdsprosessen i Kommisjonen der denne får vedtakskompetanse etter EØS-relevant personvernregelverk. Både Datatilsynet og regjeringa prioriterer deltaking i internasjonalt personvernarbeid. På denne måten kan Noreg arbeide for løysing av personvernutfordringar på den måten Noreg meiner utfordringane bør løysast, og for varetaking av personvernomsyn slik Noreg meiner det best kan gjerast. Datatilsynet må prioritere ressursar for å delta i det internasjonale personvernarbeidet, både i drøftingar med personvernstyremaktene i andre land og med store internasjonale verksemder som påverkar personvernet til innbyggjarane, som Facebook og Google. Sektorstyremaktene må òg vere medvitne om ansvaret dei har for å ta vare på personvern i sin eigen sektor, og det er derfor viktig at dei prioriterer å ta del i internasjonalt personvernarbeid, til dømes i helsesektoren og utdanningssektoren.

Noreg skal vere ein relevant og interessant deltakar og bidragsytar i det internasjonale personvernarbeidet. God nasjonal samordning av Noregs internasjonale personvernengasjement er nødvendig for å oppnå dette. Gjennom godt nasjonalt forarbeid kan utbyttet av det internasjonale samarbeidet aukast.

Boks 3.1 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.

4 Proporsjonalitet og avveging av ulike samfunnsomsyn

4.1 Generelt om vurderinga av behandling av personopplysningar i det offentlege

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. Normalt inneheld vurderinga ulike alternative løysingar. Vidare kan ein ofte setje i verk ulike tiltak for å minske ulemper og utnytte fordelar ved dei alternative løysingane. Som eksempel kan ein nemne tilgangskontroll som tiltak for å hindre unødvendig spreiing av personopplysningar i pasientjournalar og klientbasert logging (òg kalla innsynslogging) som tiltak for å motverke såkalla «snoking». Problemstillingar rundt tilgangskontroll og klientbasert logging blir omtala nærmare i kapittel 9.6.

Noreg er eit velferdssamfunn, og det offentlege har eit stort ansvar for å drive tenesteyting til folket. For å sikre innbyggjarane velferdstenester av god kvalitet er oppgåvene ofte gitt til forvaltninga gjennom lovverket. Lovverket stiller òg gjerne krav til sjølve tenesteytinga, til dømes premissar som må vere til stades for at innbyggjaren skal ha rett på ytinga.

Det er nødvendig for forvaltninga å kunne samle inn og registrere informasjon om innbyggjarane for å kunne fastsetje rettane og pliktene deira. Sakbehandlingsreglane i forvaltningslova stiller òg krav til at ei sak skal vere så godt opplyst som råd er, og det fører igjen med seg at informasjon, medrekna personopplysningar, blir innsamla, registrerte og behandla. Behandling av personopplysningar kan vere ein nødvendig føresetnad for at forvaltninga kan drive saksbehandling og tenesteyting, men er sjeldan noko mål i seg sjølv. 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.

4.2 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. Behandling av helseopplysningar i samband med helsehjelp har såleis heimel i lov. Journalen dokumenterer helsehjelpa og skal vere tilgjengeleg for helsepersonell som treng han når dei yter helsehjelp.

Ei operativ og velfungerande informasjonsforvalting i helse- og omsorgstenesta skal vere med å dokumentere gitt helsehjelp, betre kvaliteten på diagnostikk og behandling og styrkje kunnskapsgrunnlaget for førebyggjande arbeid. Dette inneber at informasjonsforvaltinga skal gjere sitt til å ta vare på grunnleggjande pasienttryggleik.

Det er ei utfordring at dokumentasjonen inneheld store mengder sensitive 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. Desse to interessene kan dra i ulike retningar. I ei velfungerande helse- og omsorgsteneste gjer dei denne typen avvegingar dagleg og på mange ulike nivå. Målet er å finne ein god balanse mellom desse interessene. 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. Viktigast er kan hende at det er mogleg å logge oppslag for å førebyggje såkalla «snoking», effektive system for tilgangskontroll og at det er mogleg å kryptere opplysningar. Dette blir nærmare drøfta i kapittel 9.5 og 9.6.

Hovudtyngda av opplysningane som blir behandla i helse- og omsorgstenesta, er underlagd teieplikt etter helsepersonellova og forvaltningslova. Teieplikt er viktig, mellom anna for å ta vare på tilliten mellom pasientane og helse- og omsorgstenesta.

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. God kunnskap om medisinske tilstandar og effekten av behandlinga har ikkje berre noko å seie for pasienten det gjeld, men òg for andre pasientar og samfunnet elles. Kvar einskild pasient bør ha eit reelt høve til å finne ut om behandlinga han eller ho får, er trygg, og om det er skilnader i kvalitet mellom ulike behandlingar og metodar. Regjeringa meiner at det ikkje er nokon motsetnad mellom personvern og pasientinteresser. Personvern er i stor grad eit spørsmål om at pasienten opplever respekt for integritet og menneskeverd, og er slik sett ei pasientinteresse. Både gode helsetenester og godt personvern gagnar pasienten. Dette er mellom anna kome til uttrykk i pasient- og brukarrettslova, der det følgjer av føremålsføresegna at lova skal fremje tilliten mellom pasient og helseteneste og ta vare på respekten for liv, integritet og menneskeverd hos kvar einskild pasient.

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.

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.

4.3 Kriminalitetsførebygging

Kriminalitet er eit trugsmål mot liv, tryggleik, livskvalitet og livsutfalding for den einskilde og mot samfunnet som heilskap. Omsynet til kriminalitetsførebygging veg derfor tungt ved utforminga av reglane som styrer informasjonsbehandlinga i politiet. 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).

4.4 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. Skole-

eigarar har til dømes plikt til å ha eit tilfredsstillande psykososialt skolemiljø og mange nyttar i den samanhengen systemet SWIS, som på bakgrunn av ein systematisert dokumentasjon gjer det mogleg å vedta tiltak for å betre læringsmiljøet på skolen. Til dømes nyttar Fylkeskommunane personopplysningar for å dimensjonere skoletilbodet i vidaregåande opplæring, og personopplysningar er nødvendige for skoleeigarar som har plikt til å fatte vedtak om spesialundervisning. I slike samanhangar må omsyn til personvern mellom anna bli vekta opp i mot omsynet til at elevane skal få den skolen dei har krav på. 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.

St.meld. nr. 41 (2008-2009) *Kvalitet i barnehagen* strekar under at dokumentasjon, informasjonsutveksling og dialog er ein nødvendig føresetnad for å tryggje ein god overgang frå barnehage til skule. Viss skulen får god informasjon om kvart barn før skulestart, kan dette hjelpe skulen med å leggje til rette for ein individuell læringsgang alt frå skulestart. Dokumentasjonen er eit viktig grunnlag for kontakten mellom foreldra, barnehagen og skulen. Føremålet må vere å gi eit godt utgangspunkt for tidleg og riktig innsats når barnet byrjar på skulen

St.meld. nr. 44 (2008–2009) *Utdanningslinja* strekar under at overføring av opplysningar om fråvære og karakterar frå grunnskulen til vidaregåande skule er viktig. Dette er ikkje direkte regulert i opplæringslova, men av allmenne føresegner i forvaltningslova og personopplysningslova. Hovudregelen er at slike overføringar skal ha grunnlag i samtykke. Det er derfor ei særleg utfordring om overføring kan skje med heimel i andre rettslege grunnlag dersom ein meiner dette særleg trengst, til dømes av omsyn til det beste for barnet. Det er viktig å få til gode overgangar i skulen for kvar einskild elev. Dette er omtala i Meld. St. 22 (2010–2011) *Motivasjon – Mestring – Muligheter, Ungdomstrinnet*. Der blir det særleg understreka at overgangen mellom hovudstega i læringsgangen og mellom de ulike skuleslaga er viktige fasar i læringsgangen til elevane. Overgangar har mellom anna påverknad på karakterane til elevane og dessutan på gjennomføringa deira av vidaregåande opplæring. Kampen mot fråfall i vidaregåande skule er høgt prioritert frå regjeringa. Følgjande er sagt i meldinga:

> «For å få gode overganger både fra barnetrinnet til ungdomstrinnet og fra ungdomstrinnet til videregående opplæring, er det viktig at den skolen eleven skal begynne på, får tilstrekkelig informasjon til å kunne tilrettelegge best mulig for den enkelte elev så raskt som mulig. Samtidig er dette personopplysninger som må behandles med varsomhet og i tråd med gjeldende regelverk.»

I Meld. St. 18 (2010–2011) *Læring og Fellesskap* blir det òg uttrykt at det ikkje finst reglar i opplæringslova eller barnehagelova som særskilt heimlar tilgang til opplysningar om personlege tilhøve ved overgang frå barnehage til skule, mellom grunnskule og vidaregåande skule eller mellom ulike etatar.

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.

4.5 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.

Problemstillingar knytte til teieplikt og ivaretaking av personvern dukkar opp i ei rekkje samanhengar i verksemda til Arbeids- og velferdsetaten. Dette er mellom anna sentrale tema i kompetanseplanar og haldningsskapande arbeid blant dei tilsette. Omsynet til teieplikt og personvern legg føringar for den fysiske utforminga av Nav-kontora, for organiseringa av einingane i etaten og for kjøp av nye IKT-system. Arbeids- og velferdsetatens bruk av personopplysningar til kontrollføremål blir omtala i kapittel 5.3.

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. Manglane gjeld særleg tilpassing og kontroll av tilgangar og logging av enkeltoppslag i saksmapper. Arbeids- og velferdsetaten har dei siste åra òg fått kritikk frå Riksrevisjonen for liknande tilhøve og for manglar i implementering og etterleving av det styringssystemet etaten har for IKT-sikring, og uttak og oppfølging av loggar, sist i Dokument 1 (2011-2012). Riksrevisjonen viser mellom anna til at etaten har utfordringar knytte til sletting av brukartilgangar og til avgrensing av brukartilgangar i saksbehandlingssystemet for barnebidrag.

Arbeids- og velferdsetaten arbeider planfast og langsiktig for å lukke avvik som blir påpeikte av Datatilsynet og Riksrevisjonen. Planane og tiltaka som er sette i verk, følgjer tre hovudspor. For det første blir det stilt krav til at nye IKT-system i moderniseringsprogrammet skal setje etaten betre i stand til å oppfylle krava i personsopplysningslova. For det andre har Arbeids- og velferdsetaten utarbeidd sentrale leiande dokument for personvern og informasjonssikring, som no blir implementerte i etaten. For det tredje blir det sett i verk ei lang rekkje kortsiktige tiltak.

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 følgjande absolutte krav til personvern og informasjonstryggleik:

> «Arbeids-og velferdsetaten skal oppfylle krav i personopplysningsloven med forskrifter med særlig vekt på konfidensialitet, integritet, lagring og logging.»

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. Mellom anna er alle landsdekkjande tilgangar og tilgangar til sensitive data gjennomgått og på enkelte område kraftig reduserte. Logging av oppslag og kontroll med at det ikkje blir gjort uautoriserte oppslag, er på plass for dei to IKT-systema med tilgang til mest personleg informasjon. Tilsvarande ordningar blir etablerte for fleire system i løpet av 2012 og 2013. Kostnader og verknadstid for nye tiltak må haldast opp mot at fleire av løysingane etter ei viss tid vil bli skifta ut.

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. Tilgangar er derfor avgrensa både ut frå kva rolle den tilsette har i verksemda, og ut frå geografi. Arbeids- og velferdsetaten har òg etablert logging av tryggleikshendingar i alle IKT-systema i etaten. Dei siste åra har etaten lagt ned mykje arbeid i å betre oppfølginga og kontrollen av desse systema.

Arbeids- og velferdsetaten har utarbeidd og operasjonalisert sentrale, leiande dokument for personvern og informasjonssikring. Styringssystemet er bygd opp med utgangspunkt i ein internasjonal standard. Lokal implementering av rutinane og retningslinene i dei leiande dokumenta har høg prioritet i etaten, sidan mellom anna oppgåva med å sikre tilstrekkeleg tilpassing av korleis dei tilsette får tilgangar og slettar tilgangar som ikkje lenger er i bruk, i hovudsak er eit lokalt ansvar.

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

saksområde. Elektronisk behandling av dokument fører til effektivisering av fleire prosessar i behandlinga av saker, betre kontroll med mottak av søknader og dokumentasjon frå brukarar og dessutan enklare og tryggare utveksling av dokument og informasjon mellom einingane i etaten. Dette inneber ein vesentleg reduksjon av risikoen for tap av og uautorisert tilgang til dokument med personopplysningar.

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.

Arbeids- og velferdsdirektoratet har stilt følgjande krav til behandling av personopplysningar i Arbeids- og velferdsetaten:

- Dei tilsette i etaten skal ha tilstrekkeleg kunnskap om krav i personopplysningslova som har noko å seie for arbeidsoppgåvene deira.
- Etaten skal sørgje for at all behandling av personopplysningar har eit klårt definert og dokumentert føremål, før det blir sett i verk behandling. Personopplysningane som blir nytta, skal vere tilstrekkelege, relevante, korrekte og oppdaterte.
- Behandlinga av personopplysningar i etaten skal delast inn i behandlingsområde som tek utgangspunkt i fagområde som logisk høyrer saman. Behandlingsområda er underlagde melde- og konsesjonsplikt til Datatilsynet
- Personopplysningar skal vere tilgjengelege for brukaren slik at kvar einskild sjølv kan ta vare på innsynsretten sin og vere med på å sikre kvaliteten på opplysningane, i tillegg til at Arbeids- og velferdsetaten kan bidra til aktiv brukarmedverknad.
- Etaten skal leggje til rette for gode rutinar som sikrar dei rettane brukaren har etter personopplysningslova.
- Etaten skal sikre at opplysningar er korrekte og ikkje blir lagra lenger enn det som er nødvendig for å oppnå føremålet med behandlinga, og tidsperioden etaten har heimel til å lagre opplysningane.
- Ved handtering av krav om innsyn skal etaten følgje reglane i offentleglova, forvaltningslova og personopplysningslova.
- Etaten skal sikre brukarar som er utsette for trugsmål, med skjermingskode frå Skatteetaten (kode 6 og kode 7) slik at det ikkje blir utlevert opplysningar om bustadadresse eller annan informasjon som kan avsløre kvar brukaren held til.
- Avtaler med tredjepart skal innehalde alle relevante krav til personvern, informasjonstryggleik og beredskap.
- Teieplikta gjeld for alle som arbeider for etaten. Kvar enkelt skal signere teieplikterklæringa til etaten og vere kjend med kva teieplikta inneber.
- Etaten skal ha ei organisering av arbeidsoppgåver som medverkar til reduksjon av innsyn i og tilgang til personopplysningar og til at teieplikta blir teken vare på ved behandling av personopplysningar.
- Etaten skal syte for at teieplikta blir teken vare på i samråd med brukaren, samhandlingspartnarane og andre aktørar.
- Informasjon som kjem inn under teieplikta, skal aldri utleverast utan tilstrekkeleg og klår heimel eller samtykke.
- Det skal førast ei samla oversikt i dei ulike fagmiljøa og einingane der etaten rutinemessig utleverer opplysningar som kjem inn under teieplikta.

Regjeringa ser det slik at Arbeids- og velferdsetaten er i ein god prosess med å sikre at personopplysningar blir behandla på ein trygg måte. Slik det kjem fram ovanfor, har etaten 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.

4.6 Ulike offentlege kontrollføremål

Meir og meir av rettshandhevinga i samfunnet blir lagd til offentleg forvaltning. Oppgåver som tradisjonelt har lege hos politi, påtalemakt og domstolar, medrekna det å avdekkje lovbrot og å påleggje sanksjonar, høyrer no inn under ulike forvaltningsorgan.

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.

4.6.1 Avveging mellom behovet for kontroll og rettsvern

Norsk rettstradisjon byggjer på stor tillit mellom innbyggjarane og staten. Staten legg som utgangspunkt til grunn at innbyggjarane følgjer dei rettsreglane som til kvar tid gjeld. Når det blir gjennomført tiltak overfor ein einskildperson for å føre kontroll med om vedkomande faktisk følgjer regelverket, må ein ta vare på dei allmenne rettsvernprinsippa og personvernomsyna.

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.

4.6.2 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. Kontrollorgana har i mange tilfelle rett til å hente inn store mengder opplysningar frå andre offentlege organ og tredjepartar, medrekna 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. I praksis er denne avgrensinga likevel mest av teoretisk interesse, fordi opplistinga femner særs vidt.

Ulike samfunnsinteresser har ulik vekt. Vitale interesser, som ivaretaking av liv og helse, veg normalt særs tungt. Reint økonomiske interesser veg mindre, men kan likevel få stor vekt dersom det økonomiske utslaget er stort. Reine ordensomsyn har relativt lita 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 dermed vanskeleg kan vege mot reint økonomiske eller andre målbare interesser. Vidare er det slik at personverninteressene først og fremst er individuelle, medan samfunnsinteressa er kollektiv. Dei som får personvernet krenkt, er med andre ord i mindretal.

Samtykke frå den registrerte er ofte rekna for å vere det føretrekte rettslege grunnlaget ved behandling av personopplysningar. Det er samtykke som best tek vare på sjølvråderetten til den einskilde. 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.

4.6.3 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. Han eller ho får kontroll med kva opplysningar som blir behandla, og kvar dei blir henta frå. Dermed kan vedkomande vurdere om opplysningane er relevante og tilstrekkelege for saka, og om dei har god nok kvalitet, før han gir dei frå seg. 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.

4.7 Forsking

For alle moderne samfunn er det ei stor utfordring å finne ein god balanse mellom satsing på forsking som kan utvikle ny og samfunnstenleg kunnskap og teknologi, og behovet samfunnet har for å verne seg mot moglege og utilsikta skadeverknader av forskinga. Det er òg ei stor utfordring å finne fram til metodar, vurderingar og verdiar som skal avgjere kva avgrensingar forskinga skal ha. Etisk refleksjon må derfor vere med i alle ledda i eit velfungerande forskingssystem. Her kjem òg personvernet inn.

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.

Tilgang til forskingsdata er viktig for eit ope samfunn, for læring og for styrking av rolla kunnskapen har i samfunnet. Men den generelle teknologiske utviklinga utfordrar personvernet også innan forskinga, for eksempel gjennom at det blir fleire måtar å drive kontroll og overvaking på. Dette kan påverke rettane til den einskilde forskingsdeltakaren.

Betre utnytting av forskingsdata gjer resultata meir etterprøvelege og fremjar kvaliteten i forskinga. Det er derfor eit mål i forskingspolitikken å leggje til rette for open tilgang til offentleg finansierte forskingsdata. Det blir mellom anna arbeidd for å følgje opp OECDs prinsipp og retningslinjer frå 2007 om tilgang til offentlig 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. Hovudoppgåvene til NSD er å vurdere om forskings- og studentprosjekt fyller krava i personopplysningslova og helseregisterlova med tilhøyrande forskrifter, og å gi informasjon og rettleiing til institusjonane og til kvar einskild forskar og student om forsking og personvern. NSD skal òg halde systematisk og offentleg oversikt over alle behandlingar dei har godkjent, og hjelpe den registrerte med å ta vare på rettane sine.

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. Datatilsynet kan gi konsesjon under føresetnad av at visse vilkår blir oppfylte. Slike vilkår er rettsleg bindande for forskarane. Både NSD og Datatilsynet gjer såleis vurderingar der føremålet med forskinga og det ein ønskjer å oppnå, blir vege opp imot personvernomsyn.

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. Dei det blir forska på må få informasjon som gjer at dei kan forstå forskingsfeltet, følgjene av å ta del i forskingsprosjektet og føremålet med forskinga.

Behovet for lettfatteleg informasjon til deltakarane er særleg stort viss forskinga inneber ei eller anna form for risiko for deltakarane. Deltakarane må få reelt høve til å reservere seg mot å ta del i forskinga, utan utilbørleg press eller ulemper for dei sjølve. Forskaren skal sjå til at informasjonen faktisk er forstått av informantane.

Kravet om samtykke skal førebyggje krenkingar av personleg integritet. Eit frivillig, uttrykkeleg og informert samtykke gjer det mogleg å gjennomføre forsking som inneber ein viss risiko for belastningar for den einskilde. 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. Samtykke som grunnlag for behandling av personopplysningar, er nærmare omtala i kapittel 6.4.

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. I utgangspunktet krev etterprøving av forskinga at forskaren publiserer tilstrekkeleg informasjon til at andre kan gjere prosedyrane opp att og etterprøve resultata. Kravet om fortrulegskap kan for eksempel innebere at ein må samle resultata i grupperingar eller modifisere omtalar eller verdiar for å sikre at informasjon ikkje let seg spore attende til einskildindivid eller særleg sårbare grupper. Sjølv om dette kan gjere det vanskelegare å etterprøve forskinga, er det viktig å respektere fortrulegskapen. Denne potensielle konflikten inneber at det er viktig at forskaren på førehand har tenkt igjennom kva konkrete strategiar ein kan leggje opp til for å sikre høg etisk standard, og samstundes, så langt råd er, ta vare på prinsippet om etterprøving av forsking.

4.8 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.

Skal ein finne balanserte løysingar mellom interessene til arbeidsgivaren og arbeidstakaren, må ein vege desse interessene mot einannan. Høvet arbeidsgivaren har til å setje i verk kontrolltiltak, kviler normalt på ei avveging mellom kva kontroll verksemda treng, kva karakter tiltaket har, og kor inngripande kontrollen verkar på arbeidstakaren. Det skal gjerast ei konkret vurdering i kvart tilfelle. Skal kontrolltiltaket vere lovleg, må interessa arbeidsgivaren har i å setje i verk tiltaket overstige ulempene arbeidstakaren blir påført.

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. Omgrepet sakleg grunn (sakleg føremål) femner om ei lang rekkje tilhøve. Både teknologi, økonomi, trygg-

leik, 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. For eksempel kan rusmiddeltesting av flygarar vere sakleg sjølv om det same kontrolltiltaket for kontorpersonell ikkje har sakleg grunn. Det blir òg kravd at tiltaket er eigna til å avdekkje det ein vil kontrollere, 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, det vil seie at kontrolltiltaket må stoppe når behovet eller føremålet som grunngav tiltaket, ikkje lenger er til stades.

Momenta i saklegheitsvurderinga er òg relevante i ei vurdering av om eit isolert sett sakleg kontrolltiltak fører med seg urimelege ulemper for arbeidstakarane. Dersom kontrolltiltaket fører med seg eit ikkje ubetydeleg inngrep i personleg integritet, respekt, privatliv eller liknande, er vilkåra for å gjennomføre kontrollen i utgangspunktet berre oppfylte i unntakstilfelle. Motsett skal det mykje til for at meir tradisjonelle kontrolltiltak i arbeidslivet, som tidsregistrering, tilgangskontroll, produksjons- og resultatkontroll eller kontroll i samband med konkret mistanke om straffelagde handlingar, blir rekna som urimelege.

Ved vurderinga av rimeleg samsvar må ein òg sjå på summen av kontrolltiltak i verksemda. Sjølv om eit kontrolltiltak isolert sett er i samsvar med lovkrava, kan gjennomføringa av det reknast som ulovleg dersom tiltaket fører til at ein går ut over den forsvarlege tolegrensa for arbeidstakaren eller sjølve arbeidsmiljøet, vurdert ut frå summen av tiltak i bedrifta.

Dei arbeidsrettslege reglane om kontroll og reglane i personopplysningslova om behandling av personopplysningar, må tolkast og praktiserast i lys av kvarandre. Dei arbeidsrettslege reglane inneheld den same norma for personvern som personopplysningslova byggjer på, men dei to regelsetta bruker ulike omgrep.

Kravet arbeidsretten stiller om sakleg grunn, fører normalt til at vilkåret i personopplysningslova om rettkomen interesse i å behandle personopplysningar, er oppfylt. Vilkåret om rimeleg samsvar/proporsjonalitet inneber normalt at omsynet til personvernet til arbeidstakaren må vurderast opp mot dei rettkomne interessene til arbeidsgivaren.

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. Med stilling som inneber særleg risiko, meiner ein stillingar der utøvaren rutinemessig kjem i situasjonar der konsekvensane av feil er særleg store (anten for vedkomande sjølv, for tredjepersonar eller for samfunnet), og der det må stillast særlege krav til aktsemd og merksemd. Dersom vilkåra er til stades, kan undersøkingane til dømes femne om rusmiddeltesting. 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. Det tyder at arbeidsgivaren må drøfte med dei tilsette i kva tilfelle ein kan gå ut frå at det trengst innsyn, og korleis eit slikt innsyn kan gjennomførast. Alle tilsette skal gjerast kjende med kva rutinar ein har i verksemda på dette området. Tilsvarande gjeld for bruk av kameraovervaking i samsvar med reglane i personopplysningslova.

4.9 Bokføringsplikt i handel og finans

Bokføringsplikta er regulert i bokføringslova[1] og bokføringsforskrifta[2] 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

[1] Lov om bokføring 19.11.2004
[2] Forskrift om bokføring 01.12.2004

på ein måte som syner at dei er rettkomne. Vidare er det ein føresetnad for etterkontroll at det er teke vare på dokumentasjonen.

Dei grunnleggjande bokføringsprinsippa er nærmare operasjonaliserte gjennom reglar i bokføringslova og bokføringsforskrifta. Reglane fører i mange tilfelle til at personopplysningar blir behandla. For eksempel inneber krava til innhaldet i sals- og kjøpsdokumentasjon at ein skal opplyse om partane, og det er òg reglar om dokumentasjon av løn, reise- og opphaldsutgifter m.m. som kan innebere plikt til registrering og lagring av opplysningar som kan knytast til ein einskildperson. I somme tilfelle kan dokumentasjonen innehalde ei rekkje personopplysningar.

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. Det blir stundom lagra særs detaljert informasjon om kvar kundane har vore, kva dei har kjøpt, og når dei gjorde transaksjonane. Dette er informasjon som kan seie mykje om rørslene og handlingane til den einskilde, og misbruk kan få alvorlege følgjer for den opplysningane gjeld. 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.

4.10 Samandrag og tilrådingar

Ved behandling av personopplysningar må ofte ulike omsyn vegast mot einannan, og det må gjerast ei proporsjonalitetsvurdering. Vurderinga skal synleggjerast, slik at ho kan etterprøvast og diskuterast.

Behandling av opplysningar til kontrollføremål ved utøving av offentleg myndigheit skal vere nødvendig. Det er viktig å vurdere tiltak som kan minske eventuelle ulemper for personvernet. Slike tiltak kan for eksempel vere innsynslogging, kryptering, informasjonsavgrensing og sikring av gode rutinar internt i kvart einskilt organ.

Boks 4.1 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.

5 Gjenbruk av personopplysningar

5.1 Generelt om personvernutfordringar ved gjenbruk av personopplysningar

5.1.1 Innleiing

Ønske om gjenbruk av data er eit meir og meir aktuelt tema. Datasett som er aktuelle for gjenbruk, kan innehalde personopplysningar, somme gonger òg sensitive personopplysningar.

Den teknologiske utviklinga opnar heile tida for nye måtar å behandle data på og gir enklare tilgang til data enn før. Samstundes blir det ofte lagra større mengder data, og det blir opna for nye måtar å stille saman data på. Samfunnsutviklinga kan vidare føre til at det etter ei tid viser seg tenleg å nytte innhenta materiale til nye føremål. Alle desse faktorane fører til ønske om gjenbruk av data. Slik gjenbruk er ofte 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.

5.1.2 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. Gjenbruk er med andre ord bruk ut over det som opphavleg var tanken bak innsamlinga, eller bruk hos andre enn den som først samla inn opplysningane.

Som for primærbehandlinga må ein ha eit rettsleg grunnlag (behandlingsgrunnlag) for gjenbruken. Behandlingsgrunnlag for gjenbruken kan, som for primærbehandlinga, vere lov, samtykke eller ein nødvendiggjerande grunn (sjå nærmare om behandlingsgrunnlaga i kapittel 6). Det er altså rettsleg sett ikkje nokon stor skilnad mellom primærbruk og gjenbruk. Gjenbruk er heller ikkje eit omgrep som blir nytta i personopplysningsregelverket.

Somme gonger ligg det i føremålet med innsamling av personopplysningar at opplysningane skal danne grunnlag for annan eller ny bruk. Dette kan spare ressursar hos den behandlingsansvarlege, samstundes som det kan vere praktisk for den registrerte å sleppe å gi frå seg den same opplysninga fleire gonger. 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 denne meldinga. Då følgjer den omfattande bruken allereie av det opphavlege føremålet og behandlingsgrunnlaget, og noko nytt rettsleg grunnlag (behandlingsgrunnlag) er såleis ikkje nødvendig. I slike tilfelle ligg den nye bruken som ein føresetnad i det opphavlege innsamlingsgrunnlaget. 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. Dersom den nye bruken ikkje ligg i det opphavlege rettsgrunnlaget, blir det omtala som gjenbruk i denne meldinga.

Somme gonger kan lovheimla teieplikt vere ein skranke for gjenbruk av personopplysningar. Det går fram av forarbeida til personopplysningslova at sjølv om den nye bruken ikkje er direkte i strid med det opphavlege føremålet, kan teieplikta vere til hinder for at opplysningane blir brukte til noko anna enn dei opphavleg vart samla inn for.

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. For eksempel har ein både i helse- og omsorgstenesta og i politiet reglar som opnar for bruk av innsamla personopplysningar hos ein ny behandlingsansvarleg eller til nye føremål enn innsamlingsføremålet. Når lovgivaren fastset reglar som opnar for gjenbruk av personopplysningar, vil den nye heimelen innebere eit nytt behandlingsgrunnlag. 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.

I IKT-politikken til regjeringa skil ein elles mellom vidarebruk av offentlege data og gjenbruk av data. Vidarebruk av offentleg informasjon, for eksempel kartdata, vêrdata, næringslivsinformasjon og trafikkinformasjon, blir nærmare regulert i offentleglova[1]. I personvernsamanheng er ikkje dette eit nødvendig skilje. I denne meldinga blir derfor all bruk av personopplysningar, både i privat og offentleg sektor, som ikkje er dekt av det opphavlege føremålet, eller som skal skje hos ein ny behandlingsansvarleg, omtala som gjenbruk.

5.1.3 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. I kontakt med det offentlege er det for eksempel praktisk for innbyggjarane å gi opplysningar berre éin gong. Gjenbruk kan òg gi større effektivitet i forvaltninga og raskare og meir korrekt sakbehandling, medverke til eit breiare grunnlag for saksbehandlinga og gi økonomiske innsparingar for samfunnet. Gjenbruk kan òg fremje interessene og rettane 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. Det følgjer samstundes av dette digitaliseringsprogrammet at ein skal ta personvernomsyn i digitaliseringsarbeidet, sjå digitaliseringsprogrammet kapittel 2. Regjeringa uttalar òg i den politiske plattforma si, Soria Moria II, at «felles infrastruktur som gir en helhetlig kontaktflate for brukere og tilrettelegging for gjenbruk av offentlige informasjonsressurser» skal liggje til grunn for IKT-politikken.

Gjenbruk kan vidare vere viktig for å sikre samfunnsinteresser. Dette gjeld særleg gjenbruk til kontrollføremål, for eksempel ved at politiet får tilgang til opplysningar i arbeidet mot kriminalitet.

Gjenbruk av opplysningar kan òg vere av interesse for private aktørar. Private aktørar kan sjå nye måtar å nytte data på, og gjenbruk kan opne for utvikling av nye tenester og verdiskaping i samfunnet. I forsking kan òg gjenbruk av opplysningar vere positivt, for eksempel gi auka kvalitet på forskinga.

Sjølv om gjenbruk av personopplysningar i mange samanhengar er både nyttig og nødvendig, reiser det likevel særlege spørsmål om ivaretaking av personvernet. Dette kan blant anna vere spørsmål om ein skal gi informasjon, og korleis ein eventuelt skal gi dei registrerte informasjon om den nye behandlinga, om dei skal få høve til å reservere seg mot den nye behandlinga, og korleis ein skal sikre at opplysningane er oppdaterte og har riktig kvalitet for det nye føremålet, slik at saksbehandlinga blir korrekt. 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. For eksempel kan det hende at den registrerte ikkje alltid har same interessa av behandlinga som ved primærregistreringa, og i somme tilfelle kan gjenbruk òg vere i strid med interessa til den registrerte. Vidare står ikkje gjenbruk av personopplysningane alltid fram for den registrerte som ei naturleg følgje av registreringa. Gjenbruk kan òg stille særlege krav til sikring av datakvalitet og varsling til den registrerte.

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».

Dette er ei naturleg følgje av grunntanken om sjølvråderetten til den einskilde og må reknast som eit viktig utgangspunkt for å ta vare på personverninteressene og kontrollen den einskilde har med spreiing av eigne opplysningar. 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.

5.1.4 Særleg om lovfesta rett til gjenbruk

Gjenbruk av personopplysningar er ofte 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 behand-

[1] Lov 19.05.2006 nr. 16 om rett til innsyn i dokument i offentleg verksemd

ling frå alle dei registrerte kan vere krevjande og i mange tilfelle òg lite tenleg. Ein kan òg tenkje seg tilfelle der den registerte 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 særskilt lov som regulerer behandlingsmåten*», jf. personopplysningslova § 5. Reglane i personopplysningslova vik såleis for reglar i andre lover om behandling av personopplysningar. 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. EMK skal ved motstrid gå føre føresegner i anna lovgiving, jf. menneskerettslova § 3. Den vurderinga av kor nødvendig inngrepet er, som EMK nemner, set dermed enkelte ytre grenser for lovgivaren.

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, og det er òg utarbeidd ei eiga rettleiing til utgreiingsinstruksen om vurdering av personvernkonsekvensar, utgitt av Fornyings-, administrasjons- og kyrkjedepartementet i 2008. Regjeringa meiner dette er viktige tiltak for å sikre eit godt personvern i alle samanhengar der ein vurderer lovfesting av behandling av personopplysningar.

5.2 Kriminalitetsførebygging

5.2.1 Utfordringar ved gjenbruk av informasjon innhenta av politiet

Politiet hentar inn mange personopplysningar som eit ledd i innsatsen mot kriminalitet. Dette gjer at opplysningane skil seg frå informasjon innhenta av andre forvaltningsorgan. Politiet hentar ofte inn opplysningar ved bruk av tvangsmiddel, medrekna hemmelege metodar. 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. Dette kan for eksempel gjelde når den som er sikta i ei straffesak, gir opplysningar til politiet.

Desse særeigne tilhøva når politiet hentar inn informasjon, fører med seg at opplysningane ofte er meir usikre enn hos andre forvaltningsorgan. Kvalitetssikring av opplysningar er derfor ei viktig oppgåve for politiet. Kvalitetssikring av opplysningar har òg 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. Dette er eit verkemiddel som skal sikre personvernet, slik at ufullkomen informasjon som er registrert hos politiet, ikkje blir ukritisk nytta av andre organ eller personar.

5.2.2 Gjenbruk av informasjon innhenta som forvaltningsorgan

Ei særleg utfordring for personvernet i politisektoren er at politiet fører register både over forvaltningsoppgåver og over arbeid med oppklaring av straffesaker. I forlenginga av dette kan det 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. For eksempel kan opplysningane i passregisteret som hovudregel berre nyttast til å gjennomføre reglane i passlova. 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.

5.2.3 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. Denne særskilde teieplikta inneber ei avgrensing av kva føremål ein kan gjenbruke opplysningane til, fordi opplysningane berre kan nyttast som prov i den straffesaka som tvangsmiddelet er kravd som ledd i. Dersom ein ved bruk av tvangsmiddelet finn bevis for andre lovbrot òg, kan opplysningane berre nyttast dersom det gjeld eit lovbrot som kan grunngi den typen tvangsmiddel som beviset vart funne gjennom.

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. Fleirtalet i utvalet uttalar mellom anna følgjande om avveginga mellom kriminalitetsførebygging og personvern:

> «Utvalgets flertall har, etter en samlet vurdering av de hensyn som taler henholdsvis for og imot å begrense adgangen til bruk av overskuddsinformasjon som bevis, kommet til at dagens generelle begrensning til saker som i seg selv kunne begrunnet den aktuelle tvangsmiddelbruken, bør oppheves. I tilfeller der et bevis er innhentet på lovlig vis som ledd i etterforsking og klart viser at mistenkte har begått en straffbar handling, kan hensynet til mistenktes personvern ikke rettferdiggjøre avskjæring av beviset.»

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

5.3 Bruken av personopplysningar for kontrollføremål i Arbeids- og velferdsetaten

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 proposisjonen, Ot.prp. nr. 76 (2007–2008), heiter det mellom anna følgjande:

> «Ein del av høyringsinstansane er opptekne av at reglane om opplysningsplikt må ha som grunnlag ei prinsipiell vurdering av tilhøvet mellom personvern og behovet for å avdekkje trygdemisbruk. For hovuddelen av reglane om opplysningsplikt og for hovuddelen av tilfella der det er behov for å be om opplysningar, er likevel problemstillinga ei noka anna. Arbeids- og velferdsetaten administrerer eit sett av ytingar som Stortinget har vedteke og som byggjer på at ytingane skal gå berre til dei som fyller vilkåra for dei. For å kunne avgjere dette, er det nødvendig med opplysningar, og det er òg nødvendig med kontroll for å unngå at stønadsordningane kjem i vanry. I tilsvarande grad må personvernet vike, og dette vil oftast bli opplevd som naturleg og nødvendig av dei som har sett fram krav om ytingane. Dersom ein som har sett fram krav om uførepensjon ikkje ønskjer at etaten skal få tilgang til helseopplysningane sine, vil den einaste utvegen vere å gi avkall på ytinga. Dette kan ikkje vere annleis dersom trygdesystemet skal kunne fungere som trygdesystem. På den andre sida skal Arbeids- og velferdsetaten som nemnd ikkje ha andre opplysningar enn dei som etaten treng for å utføre oppgåvene sine, men dette behovet er annleis og større i misbrukssaker enn i vanlege stønadssaker.
>
> Arbeids- og inkluderingsdepartementet er samd i at balansegangen mellom personvernomsynet og omsynet til å hindre eller avdekkje trygdemisbruk er vanskeleg. Det er òg slik at høyringsnotatet i liten grad fokuserer på dette. Årsaka til dette er likevel i alt vesentleg at forslaga faktisk ikkje var meint å gripe så sterkt inn i personvernet som nokre av høyringsinstansane ser ut til å tru.»

Sitatet viser nokre av dei vanskelege avvegingane mellom personvern og andre omsyn som departementet gjorde i vurderinga av tilgang til og gjenbruk av personopplysningar i kontrollverksemda til Arbeids- og velferdsetaten.

I innstillinga til Odelstinget nr. 35 (2008–2009) viser samstundes komiteen til kva velfungerande

kontroll har å seie for å ta vare på tilliten til trygdesystemet:

> «Komiteen viser til at Arbeids- og velferdsetaten står sentralt i arbeidet med å hindre og avdekke trygdemisbruk ettersom det er denne etaten som kjenner reglene og behandler sakene og derfor er nærmest til å avsløre misbruk. Komiteen understreker viktigheten av å forebygge og å avdekke trygdemisbruk for å kunne opprettholde oppslutningen om gode velferdsordninger.»

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.

5.4 Marknadsføring

Marknadsføringsreglane krev i dag at det skal hentast inn samtykke før elektronisk utsending av direkte marknadsføring. Eksempel på direkte marknadsføring er marknadsføring retta mot forbrukarar ved hjelp av telefon, adressert post, e-post, SMS eller elektroniske meldingar sende gjennom sosiale medium. Ved marknadsføring ved hjelp av telefon eller direkteadressert post er det ikkje krav om førehandssamtykke. I desse tilfella finst det ei reservasjonsordning som kan nyttast av forbrukarar som ikkje ønskjer slike førespurnader.

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. Auken i elektronisk kommunikasjon og framveksten av nye kanalar har samstundes gjort det viktigare for brukarane at den elektroniske kommunikasjonen fungerer godt og ikkje blir uroa av uønskte førespurnader. Krav som pålegg næringsdrivande å hente inn samtykke før dei vender seg direkte til personar gjennom dei elektroniske kommunikasjonskanalane dei nyttar, er derfor heilt nødvendig.

Med det jamt aukande talet på næringsdrivande forbrukarane kommuniserer elektronisk med, blir det òg 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. Eit eksempel er ei sak der Marknadsrådet etter påstand frå Forbrukarombodet, påla ei møbelkjede å betale eit straffegebyr på 150 000 kroner for å ha sendt ut reklamemeldingar på SMS til 152 000 personar (MR-sak 11/685). Mobilnummera til desse 152 000 personane var innsamla over ein periode på ni år, med det føremålet å kunne kontakte personane når møblar dei hadde tinga, var ferdige til levering. Den næringsdrivande valde likevel å nytte opplysningane til å rette direkte marknadsføring mot personar som ikkje hadde samtykt i det. Reglane i personopplysningslova var brotne ved at desse telefonnummera vart lagra lenge etter at føremålet med innhentinga var gjennomført.

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. I mai og juni 2011 vart for eksempel 2300 forbrukarar fakturerte for til saman 2,2 millionar kroner (200 kr per motteken SMS) frå eit firma som sende ut overtakserte SMS-meldingar, som mottakarane ikkje hadde tinga. Dei drygt 230 personane som klaga til Forbrukarombodet i saka, visste stort sett

heller ikkje korleis personopplysningane deira hadde hamna i databasen til den næringsdrivande. Marknadsrådet gjorde vedtak om straffegebyr på kr 500 000 for firmaet som hadde sendt ut meldingane, og kr 150 000 for styreleiaren personleg (MR-sak 11/1436).

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. På grunn av den store mengda aktørar i marknaden er det likevel ei vanskeleg oppgåve å nå ut til alle med informasjon og hindre at det skjer lovbrot.

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. Det er derfor enkelt for alle som ønskjer å drive marknadsføring ved hjelp av telefon eller post å få tilgang til opplysningane dei treng for å kunne gjennomføre dette. Trass i ordninga med reservasjonsregisteret, viser klagesaker til Forbrukarombodet at ei rekkje næringsdrivande og humanitære organisasjonar kontaktar personar som har reservert seg. Ein kan derfor spørje om det er for lett tilgang til dei opplysningane som trengst for å gjennomføre marknadsføringa.

5.5 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.

Gjenbruk av helseopplysningar er avgjerande for å kunne halde oversikt over førekomsten av ulike sjukdomar og for forsking på sjukdomsårsaker og behandlingseffektar. Slik kunnskap er ein føresetnad for at kvar einskild pasient skal kunne gjere gode sjølvstendige val, og er viktig for retten pasientane har til likeverdige helsetenester.

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. Dette er fordi alternativet ofte er å hente inn opplysningar manuelt, anten frå journalsystem eller frå pasientane. Eit register kan leggje til rette for betre kvalitet, færre tilgjengelege opplysningar (avgrensa til dei som er relevante og nødvendige), mindre overskotsinformasjon og mindre behov for direkte personidentifikasjon.

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. Dette kjem mellom anna av at både det potensielle inngrepet i personvernet og den konkrete nytta for den einskilde registrerte kan vere lite synleg. 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. Konsekvensen av denne typen mangel på representativitet kan vere at registra ikkje er eigna til å oppfylle det føremålet dei er oppretta for å ta vare på. Erfaringa viser at dei sjukaste pasientane ofte er for dårleg representerte i samtykkebaserte register. Ein kan gå ut frå at mange som ikkje aktivt går til det steget å samtykkje, i grunnen ønskjer å vere med på denne typen samfunnsnyttige oppgåver. Manglande deltaking kan i mange tilfelle kome av at den potensielle respondenten mistar eller rotar bort informasjonsskrivet eller samtykkefråsegna, og at vedkomande derfor ikkje blir inkludert. Stortinget har lagt til grunn at enkelte sentrale helseregister ikkje bør tuftast på samtykke fordi eit samtykkekrav fører til problem 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. Gjenbruk må gi så låge personvernkostnader som råd er. Opplysningane bør avidentifiserast eller anonymiserast så langt det er mogleg, utan at det kjem i vegen for føremålet med registreringa. Vidare må rettane til den registrerte, mellom anna retten til innsyn og retting, tryggjast. Det bør òg leggjast til rette for at den registrerte kan reservere seg mot oppføring i visse register.

5.6 Forsking

5.6.1 Forsking og kunnskapsbehovet i forvaltninga

I kraft av si rolle som tenestetilbydar lagrar forvaltninga store mengder personopplysningar. Desse personopplysningane er nødvendig informasjon som er innhenta som eit ledd i tenesteytinga. Arkivlova stiller krav om at materialet skal oppbevarast, og opplysningsmassen utgjer eit svært godt utgangspunkt for å få ny kunnskap.

Ved å analysere dei innsamla personopplysningane og nytte dei som statistikkgrunnlag eller som utgangspunkt for mellom anna kvalitetssikring, kvalitetsutvikling og forsking, kan samfunnet skaffe seg uvurderleg og nødvendig kunnskap om dei ulike tenestesektorane.

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. Personeintydige opplysningar vil ofte vere knytte til fødselsnummeret til personen. For mange føremål er utvalsundersøkingar og statistikk på aggregert nivå tilstrekkeleg for å oppfylle det behovet staten har for informasjon. På andre område talar viktige omsyn for at personeintydige opplysningar bør samlast inn og behandlast på sentralt nivå. Fleire av dei sentrale helseregistra er eksempel på dette.

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. Anonymiserte data inneber at namn, fødselsnummer og andre personeintydige kjenneteikn er fjerna, slik at opplysningane ikkje lenger, korkje direkte eller indirekte, kan knytast til ein enkeltperson.

5.6.2 Fordelar og utfordringar ved gjenbruk

Gjenbruk av personopplysningar må ha eit eige behandlingsgrunnlag. Både mindre forskingsprosjekt og større statistiske analysar må oppfylle reglane i personopplysningslova eller eventuelt helseregisterlova eller helseforskingslova.

For forskingsprosjekt vil det ofte vere nødvendig med dispensasjon frå teieplikta for å få tilgang til informasjonen. Teieplikta etter forvaltningslova § 13 og helsepersonellova (som gjeld helseopplysningar) er med på å ta vare på personvernet til innbyggjarar som på ulike måtar er i kontakt med forvaltninga.

Statistikk basert på personeintydige opplysningar er i mange tilfelle meir kostnadseffektiv enn statistikk basert på ulike aggregerte nivå og utvalsundersøkingar. Det kjem blant anna av at det som regel er mindre administrativt krevjande å rapportere personeintydige opplysningar som allereie er registrerte. Dei fleste utvalsundersøkingar er på si side svært kostbare å gjennomføre, både økonomisk og administrativt. 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. Det er òg effektiv samfunnsøkonomi at allereie innsamla informasjon blir nytta til fleire føremål.

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. Gjenbruk kan medføre spreiing av personopplysningar ut over det som var utgangspunktet for det opphavlege behandlingsgrunnlaget. Det kan òg medføre at fleire får tilgang til personopplysningar, sjølv utan at det er ein direkte fordel for individet eller står i direkte samband med tenesteytinga.

Både statistikk og forskning er i personopplysningslova vurderte som legitime behandlingsføremål. Det følgjer av personopplysningslova § 11 andre leddet at

> «[s]enere behandling av personopplysningene for historiske, statistiske eller vitenskapelige formål anses ikke uforenlig med de opprinnelige formålene med innsamlingen av opplysningene, jf. første ledd bokstav c, dersom samfunnets interesse i at behandlingen finner sted, klart overstiger ulempene den kan medføre for den enkelte».

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:

- Forskingsprosjekta kan gi meir kunnskap om sjukdomar og førebygging av sjukdomar som kan kome den enkelte registrerte til gode (sjå det Personvernnemnda har uttala, særleg i sak 2002-06 SIRUS).
- Forskingsprosjekta kan bidra til utvikling av allmennyttig medisinsk kunnskap
- Det vil til kvar tid bli gjennomført forskingsprosjekt. Det må leggjast vekt på den økonomiske innsparinga ved å bruke den eksisterande koplingsbrua i staden for å opprette nye (ein kostnad på mellom ein kvart og ein halv million kroner per bru).
- Forsking (vitskaplege føremål) er særleg nemnd i personopplysningslova og må derfor i interesseavveginga reknast som eit særleg viktig føremål for samfunnet.

Vurderinga her 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.

5.7 Gjenbruk av opplysningar i arbeidslivet

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 behandlingsansvarlege. Hovudregelen i tvistemålslova er fri bevisføring. Retten kan likevel i særlege tilfelle nekte føring av bevis som er skaffa på utilbørleg måte. Når det kjem krav om at opplysningar som er skaffa gjennom kontrolltiltak, ikkje skal kunne leggjast fram som bevis, må retten direkte eller indirekte ta stilling til om kontrolltiltaket er rimeleg, og om det inneber ei krenking av personvernet.

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. Arbeidsgivaren kan kontrollere på ein meir inngripande måte i ei enkeltsak når det finst mistanke, enn han kan ved rutinekontroll.

Skjult overvaking, for eksempel hemmeleg kameraovervaking, blir normalt rekna som ulovleg. Tilsvarande gjeld provokasjonsliknande tiltak. I rettspraksis (blant anna Rt. 1991 s. 616 *Gatekjøkkendomen*) er slike tiltak vurderte som ei grov krenking av grunnleggjande personvernomsyn, og retten har ikkje godteke at resultat frå desse tiltaka skulle leggjast fram som bevis.

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. Retten er då komen til at bevisa ikkje krenkjer grunnleggjande personvernomsyn, og at det er viktig at dei blir framlagde av omsyn til faktum i saka. Graden av krenking har såleis noko å seie for bevisavskjeringa.

Det er framleis etter måten lite rettspraksis på området, og det er vanskeleg å trekkje klåre konklusjonar.

5.8 Dokumentasjonsplikt og dokumentasjonsbehov for ettertida

5.8.1 Tilhøvet til ulike oppbevaringsplikter

Arkivlova og pliktavleveringslova inneheld reglar om bevaring og tilgjengeleggjering av allereie produsert, og til dels tilgjengeleggjort, materiale. Arkivlova regulerer bevaring av alle offentlege arkiv og somme privatarkiv. Pliktavleveringslova regulerer avleveringsplikt for allment tilgjengelege dokument.

Ingen av lovene pålegg dokumentproduksjon, dei regulerer berre bevaring av allereie produsert 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. Både arkivlova og pliktavleveringslova er derfor avgjerande for at ein skal kunne sikre ytringsfridom og rettstryggleik. Dokumentasjonsbevaring er òg ein avgjerande føresetnad for å kunne dokumentere samtida i ettertida.

5.8.2 Arkivregelverk

Føremålet med arkivlova er å

> «tryggja arkiv som har monaleg kulturelt eller forskingsmessig verde eller som inneheld rettsleg eller viktig forvaltningsmessig dokumentasjon, slik at desse kan verta tekne vare på og gjorde tilgjengelege for ettertida», jf. § 1.

Arkivlova gjeld i all hovudsak for offentlege institusjonar. Privatarkiv er omfatta av regelverket berre i ein viss grad. Dersom eit privatarkiv skal vere arkivpliktig etter arkivlova, må det gjerast eit særskilt vedtak om dette med heimel i arkivlova § 19.

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. Eventuelle avslag på førespurnader om innsyn skal grunngivast. I gjeldande offentleglov er det ikkje sett noka grense for kor langt tilbake i tid innsynsretten gjeld. Det følgjer av dette at også arkivdepotinstitusjonane som hovudregel må ha ein heimel i offentleglova eller i forskrifta til den dersom dei avslår innsyn. Eit eventuelt avslag må grunngivast i relevante reglar.

Alle arkiv er pålagde å rette seg etter teiepliktreglane som er fastsette i ei rekkje ulike lover. I praksis inneber dette at tilgjengeleggjering av arkivmateriale er avhengig av kva reglar som eventuelt avgrensar tilgangen. Generelle reglar om teieplikt for offentlege tenestemenn er gitt i forvaltningslova. Ei rekkje særlover inneheld eigne reglar om teieplikt. Både forvaltningsorgana og enkelte arkivdepot oppbevarer dokument med opplysningar som er graderte etter tryggingslova, og dette inneber både teieplikt og særlege krav til vern av opplysningane.

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. Påbodet om at arkivdepota skal sikre tilstrekkeleg fortruleg behandling, medfører blant anna at arkivmateriale som gjer det mogleg å søkje på namn på personar som er i live, ikkje skal leggjast ut på nettet.

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.

5.8.3 Pliktavleveringslova

Føremålsparagrafen i pliktavleveringslova stiller opp ei ramme for kva materiale som skal pliktavleverast. Føremålet med lova er

> «å tryggja avleveringa av dokument med allment tilgjengeleg informasjon til nasjonale samlingar, slik at desse vitnemåla om norsk kultur og samfunnsliv kan verta bevarte og gjorde tilgjengelege som kjeldemateriale for forsking og dokumentasjon», jf. § 1.

Det er altså 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.

Personvernkommisjonen skreiv i NOU 2009: 1 *Individ og integritet*:

> «Nasjonalbibliotekets tilnærming til elektronisk pliktavlevering, der et elektronisk dokument som blir gjort offentlig tilgjengelig på Verdensveven automatisk blir lastet ned og arkivert, bør diskuteres. Lovhjemmelen bør gjennomgås og avlevering av alle elektroniske dokumenter fra nettet bør reguleres i lov eller eventuelt i forskrift. Det bør foretas en utredning av hvordan dette skal skje og hvilke elektroniske dokumenter det skal avgrenses mot, samt hvordan dette skal gjøres.»

Kulturdepartementet er i gang med ein revisjon av pliktavleveringslova og skal som ledd i denne prosessen blant anna sjå på korleis pliktavlevering frå internett bør gjennomførast.

5.9 Samandrag og tilrådingar

Tilrettelegging for gjenbruk av data er ein viktig del av politikken til regjeringa, og det skal i størst mogleg grad leggjast til rette for gjenbruk av offentlege informasjonsressursar. Der data inneheld personopplysningar, må ein likevel vere varsam. Slike data skal berre gjenbrukast dersom ei vurdering av om gjenbruk er nødvendig, viser at det er gode grunnar til det.

Dataminimalitet er eit viktig personvernprinsipp. Anonymisering eller anna avidentifisering av personopplysningar og andre avhjelpande tiltak bør derfor vurderast ved gjenbruk av personopplysningar.

Lovreglar som heimlar rett til gjenbruk av innsamla personopplysningar, bør vere så presise som mogleg, slik at det lèt seg gjere for dei registrerte å forstå at opplysningar kan bli brukte til nye formål.

Mange opplever bruk av personopplysningar som grunnlag for direkte marknadsføring som eit personverninngrep. Tilsynet med korleis næringsdrivande lagrar og bruker personopplysningar til marknadsføring, vil bli vurdert i samband med evalueringa av marknadsføringslova.

Ved oppretting av helseregister må ein gjere ei avveging mellom behova samfunnet har, nytta av gjenbruken og den registrerte sitt behov for personvern. Det bør i størst mogleg grad bli lagt til rette for at den registrerte kan reservere seg mot oppføring i register.

Regjeringa vil vurdere å utarbeide ei klårare regulering av retten ein arbeidsgivar har til å gjenbruke opplysningar om ein arbeidstakar til andre føremål enn det dei opphavleg var innhenta for.

Boks 5.1 Hovudpunkt kapittel 5

- 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.

6 Vilkår for behandling av personopplysningar

6.1 Generelt om det rettslege grunnlaget for behandling av personopplysningar

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 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.

Boks 6.1 Kva er sensitive personopplysningar

Etter personopplysningslova er sensitive personopplysningar opplysningar om
- rasemessig eller etnisk bakgrunn eller politisk, filosofisk eller religiøs oppfatning
- at ein person har vore mistenkt, sikta, tiltala eller dømd for ei straffbar handling
- helse
- seksualitet
- medlemskap i fagforeiningar

Også tilsynelatande trivielle opplysningar, som til dømes adresse, kan somme gonger røpe sensitiv informasjon. Dette er blant anna tilfellet for personar som har adresse i fengsel eller i helseinstitusjon.

Andre opplysningar enn dei som lova definerer som sensitive, kan vere opplysningar den registrerte ønskjer å verne. Dette kan til dømes vere opplysningar om økonomiske tilhøve, som mange oppfattar som sensitive. Desse opplysningane er likevel ikkje underlagde det særlege vernet personopplysningslova gir for sensitive personopplysningar.

6.2 Val av behandlingsgrunnlag

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

framheva som det føretrekte grunnlaget for behandling, i alle fall der dei registrerte har eit reelt val.

I valet mellom samtykke eller nødvendiggjerande grunn som grunnlag for behandling av personopplysningar, går det fram av forarbeida til personopplysningslova[1] at personopplysningsbehandlingar i størst mogleg grad bør baserast på samtykke der dette let seg gjere. At den registrerte har kontroll med flyt og bruk av opplysningar om seg sjølv, er grunnleggjande for bruk av andre rettar etter personopplysningsregelverket. Samtykke legg til rette for slik kontroll.

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. Den offentlege tenesta kan vere lovregulert og innebere behandling av personopplysningar, som tenesteyting i arbeids- og velferdsforvaltninga eller i skulesektoren, utan at behandlinga er nærmare omtala i regelverket. Slik tenesteyting blir òg utført av private aktørar. Det vil som regel ikkje vere riktig å la samtykke vere grunnlag for behandling av personopplysningar som er ein nødvendig føresetnad for å kunne ta imot ein lovheimla rett, eller som er nødvendig for utøving av andre lovregulerte oppgåver.

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. I slike tilfelle er det til no ikkje vurdert som nødvendig å basere behandlinga på samtykke. At ein ikkje *trur* at dei registrerte vil gi sitt samtykke til behandlinga, er derimot som hovudregel *ikkje* eit argument for å velje å basere ei personopplysningsbehandling på eit anna rettsleg grunnlag enn samtykke. Tvert imot kan dette, særleg i privatrettsleg samanheng, haldast for å vere eit godt argument for at behandlinga nettopp bør baserast på samtykke frå dei registrerte.

[1] Ot.prp. nr. 92 (1998-99)

6.3 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.

Samtykke er eit lite eigna behandlingsgrunnlag for dei fleste behandlingar av personopplysningar i forvaltninga. Det er for eksempel lite praktisk at innbyggjarane skal kunne setje fram krav om ei yting eller teneste, men samstundes ha rett til å nekte at opplysningar om dei blir behandla for å avgjere om tenesta skal ytast, og i kva omfang. Barnevernet er eit døme på ei offentleg teneste som gjer det nødvendig å behandle personopplysningar utan grunnlag i samtykke. Barnevernet skal sikre at barn og unge som lever under forhold som kan skade helsa og utviklinga deira, får nødvendig hjelp og omsorg til rett tid. For å løyse oppgåvene sine må barnevernet kunne behandle sensitive personopplysningar uavhengig av om foreldra samtykkjer i det.

Somme lover regulerer sjølve behandlinga av personopplysningar, og behandlinga kan stå fram som eit mål i seg sjølv. Helseregisterlova er eit godt eksempel på ei slik lov. Ho gir eit fullt sett med reglar om behandling av helseopplysningar i helse- og omsorgssektoren som langt på veg erstattar personopplysningslova på dette området.

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. Behandling av personopplysningar er sjeldan noko mål i seg sjølv, men berre eit middel for å realisere eit mål. Til dømes er det ein føresetnad at skulen kan behandle opplysningar om elevane for å gi dei den undervisninga dei har krav på. Det vil vere unødvendig tungt og lovteknisk krevjande om lovheimlane i detalj skal regulere kva opplysningar ein kan hente inn, og korleis ein kan behandle dei for at forvaltninga skal kunne ta seg av dei lovpålagde oppgåvene sine.

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. Behandling av sensitive personopplysningar treng klårare heimel enn behandling av meir trivielle personopplysningar. Til dømes vil behandling av personopplysningar til kontrollføremål i arbeids- og velferdsforvaltninga krevje klårare heimel enn når plan- og bygningsetaten behandlar personopplysningar i byggjesaker.

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. Det er mange offentlege oppgåver som føreset behandling av personopplysningar, og behandlingane vil derfor ofte vere nødvendige for å utøve offentleg myndigheit. Likevel er det ikkje knytt lovheimla rett til å behandle personopplysningar til alle desse offentlege oppgåvene. I slike tilfelle må forvaltninga kunne behandle personopplysningar med heimel i personopplysningslova § 8 bokstav e. Vilkåret seier at ein kan behandle personopplysningar når det er nødvendig for «å utøve offentlig myndighet». Dette er meint å omfatte både situasjonar der offentlege organ gjer vedtak, i tillegg til utøving av meir administrative funksjonar for å ta vare på rettane og pliktene til innbyggjarane. Er opplysningane og behandlinga nødvendig for at styremaktene skal kunne utføre desse lovpålagde oppgåvene, vil behandling derfor oppfylle kravet i personopplysningslova § 8 bokstav e.

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. Forvaltningsorgan kan behandle dei personopplysningane som er nødvendige for å gjere enkeltvedtak eller ta andre avgjerder som ledd i å utøve offentleg myndigheit. 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.[2]

[2] Bygrave/Schartum Personvern i informasjonssamfunnet 2. utgåva s. 164-165

Det som er sagt ovanfor, inneber at forvaltninga si behandling av personopplysningar i hovudsak vil ha lovheimel eller vere nødvendig for utøving av offentleg myndigheit. Private aktørar si behandling av personopplysningar i samband med utøving av lovpålagde oppgåver vil som hovudregel òg ha lovheimel. Det kan likevel vere tilfelle der andre behandlingsgrunnlag, for eksempel samtykke, er relevante, typisk i tilfelle der forvaltningsorganet er utanfor kompetanseområdet sitt.

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. Som lovheimel reknar ein òg reglar som har som føresetnad at det vert behandla personopplysningar som er nødvendige for å oppfylle eit føremål. 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.

6.4 Samtykke som behandlingsgrunnlag

Samtykke blir i mange samanhengar framheva som det føretrekte grunnlaget for behandling av personopplysningar. Dette er óg stadfesta i internasjonal rett. Samtykke som behandlingsgrunnlag gjeld særleg i privat sektor, der det sjeldan vil vere lovheimel for ei behandling. Brukt riktig vil samtykke som behandlingsgrunnlag kunne gi grunnlag for godt personvern.

6.4.1 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 der vedkomande klårt og tydeleg godtek å vere del av ei personopplysningsbehandling. 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. Dersom det kan vere tvil om den registrerte opplever å ha eit reelt val, bør ikkje behandling av personopplysningar ha grunnlag i samtykke. Eit døme kan vere tilhøvet mellom ein arbeidsgivar og ein arbeidstakar, der arbeidsgivaren normalt vil ha ein vesentleg sterkare posisjon enn arbeidstakaren. Arbeidstakaren kan oppleve eit press for å godta arbeidsgivaren sine vilkår. Tilsvarande kan gjelde ved utøving av offentleg myndigheit, der behandling av personopplysningar kan vere heilt nødvendig for å tryggje rettane og pliktene til innbyggjaren. I slike samanhengar opplever den registrerte at han eller ho ikkje har noko val, og samtykket tilfredsstiller neppe krava i personopplysningslova. Innhaldet i kravet om at samtykket skal vere frivillig, blir omtala nærmare i punkt 6.4.2.

Det kan vere grunn til å vurdere om andre former for aksept frå den registrerte enn eit eksplisitt samtykke kan seiast å tilfredsstille kravet personopplysningslova set til samtykke, og såleis kan danne grunnlag for behandling av personopplysningar. Alternativ til samtykke kan vere reservasjonsrett eller implisitt samtykke/konkludent åtferd. Reservasjonsrett (på engelsk omtala som «*opt out*») inneber at den registrerte må gjere noko aktivt for å sleppe å bli registrert, medan konkludent åtferd inneber at ein blir halden for å ha godteke behandlinga dersom ein utan protestar innlèt seg på aktivitetar som krev behandling av personopplysningar. Reservasjonsrett blir omtala i kapittel 6.5.

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. Kanskje har den registrerte ikkje reflektert over at ein aktivitet kan medføre bruk av personopplysningar, og derfor ikkje kan seiast å ha gitt samtykke til personopplysningsbehandlinga. Den behandlingsansvarlege må vurdere om ein kan forvente at dei registrerte har forstått at handlinga deira ville medføre bruk av personopplysningar.

«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. Ofte tek den behandlingsansvarlege inn vilkår om behandling av personopplysningar i standardvilkår i dette «clickwrap»-formatet. Når ein inngår avtale med til dømes ein nettbutikk, vil butikken kunne vise til at det er gitt samtykke til behandling av personopplysningar og/eller elektronisk marknadsføring på denne måten.

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. Implisitt samtykke kan derfor vere lite eigna som behandlingsgrunnlag etter personopplysningslova med mindre handlingane heilt openbert vil føre til bruk av personopplysningar.

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.

6.4.2 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.

Samtykkeutfordringar i arbeidslivet

Kontroll og overvaking av tilsette er regulert i arbeidsmiljølova[3]. Arbeidsgivaren kan berre setje i verk kontrolltiltak som har sakleg grunn i verksemda og ikkje inneber ei urimeleg belastning for arbeidstakaren. Samstundes er behandling av personopplysningar i arbeidslivet regulert i personopplysningslova med forskrifter. Personopplysningar som blir samla inn i samband med kontrolltiltak, skal behandlast i samsvar med reglane i personopplysningslova.

Samtykke som behandlingsgrunnlag kan likevel vere problematisk i arbeidsforhold på grunn av den bindinga arbeidstakaren gjerne opplever til arbeidsgivaren sin. Denne bindinga gjer at partane ikkje nødvendigvis kan reknast som «likeverdige» når samtykket blir gitt, noko som igjen vil ha sitt å seie for om samtykket er frivillig. I Personvernnemnda sitt vedtak i sak PVN 2005-06 Securitas uttrykkjer nemnda dette slik:

> «I dette tilfellet fremhever Securitas som arbeidsgiver at en nektelse ikke vil få følger for den aktuelle persons ansettelsesforhold. For den enkelte vil det likevel være nærliggende å oppleve at det vil kunne få konsekvenser for vedkommendes arbeidsforhold. Arbeidsgiver har alltid en viss makt over de ansatte gjennom sin styringsrett. Det vil i skyggen av denne være vanskelig å anse et samtykke fra en ansatt avgitt uten tanke på at nektelse vil kunne ha betydning for fremtiden – selv om arbeidsgiver ikke har til hensikt å utnytte opplysningene til skade for arbeidstaker.»

Samtykke er i mange samanhengar det føretrekte behandlingsgrunnlaget etter personopplysningslova. Systemet i arbeidsmiljølova er annleis. Reglane i arbeidsmiljølova skal verne den tilsette mot usakleg og utilbørleg overvaking og kontroll. Reglane kan ikkje fråvikast til ugunst for arbeidstakarane gjennom samtykke med mindre det er eit særskilt rettsleg grunnlag for det. Slike heimlar finst ikkje i dag, og gjeldande regelverk er derfor til hinder for at arbeidstakaren kan samtykkje i kontrolltiltak som er i strid med krava i arbeidsmiljølova kapittel 9. Individuelt samtykke er ikkje tilstrekkeleg som rettsleg grunnlag for eksempel for innhenting av helseopplysningar eller gjennomføring av medisinske undersøkingar i samband med tilsetjingar. Dette vil vere eit så alvorleg inngrep i den personlege sfæren at samtykke ikkje er tilstrekkeleg heimelsgrunnlag uavhengig av om arbeidstakaren føler seg pressa til å gi det eller ikkje. For slike tilfelle inneheld derfor arbeidsmiljølova uttømande regulering av kva opplysningar arbeidsgivaren har lov til å hente inn, og kva han kan bruke opplysningane til. Reglane i personopplysningsforskrifta om arbeidsgivaren sitt innsyn i e-posten til tilsette er òg utforma slik at dei ikkje kan fråvikast ved avtale til ugunst for arbeidstakaren. Arbeidstakaren i skal ikkje pressast til å «samtykkje» i at arbeidsgivaren får tilgang til e-postkassa.

Samstundes som arbeidsgivaren ikkje har rett til å fråvike reglane til ugunst for arbeidstakaren, er det fullt høve til å avtale kontrolltiltak innanfor rammene som følgjer av lova. Blant anna inneheld hovudavtalen mellom LO og NHO regulering knytt til kontroll- og overvakingstiltak.

I internasjonal samanheng òg blir arbeidsforhold trekte fram som døme på bindingar der samtykke vanskeleg kan bli gitt frivillig. I punkt 34 i fortalen til EUs utkast til personvernforordning er nettopp forholdet mellom arbeidsgivar og arbeidstakar brukt som døme på eit ubalansert styrkeforhold som kan medføre at samtykke ikkje er gitt frivillig, og såleis ikkje eignar seg som grunnlag for behandling av personopplysningar.

Samtykkeutfordringar i helse- og omsorgstenesta

For å behandle helseopplysningar i helse- og omsorgssektoren er utgangspunktet at ein må ha samtykke eller lovheimel. Dette er kome til uttrykk i fleire av helselovene, som til dømes pasient- og brukarrettslova og helseregisterlova. Samtykke er vidare eit sentralt element i medisinsk forskingsetikk, og kravet er derfor òg nedfelt i helseforskingslova.

Hovudregelen i helseregisterlova er at registrering og bruk av helseopplysningar til anna enn helsehjelp skal vere basert på samtykke frå dei registrerte. Samtykke er meint å sikre at den enkelte har innverknad på bruken av helseopplysningar om seg sjølv. Føring av pasientjournal føl-

[3] Lov 17.06.2005 nr. 62 om arbeidsmiljø, arbeidstid og stillingsvern mv., kap. 9

gjer likevel av lov og er ei plikt som ligg på helsepersonell når dei yter helsehjelp. Føring av journal krev ikkje samtykke frå pasienten. Det same gjeld for dei sentrale helseregistra, som har stor samfunnsnytte. For dei er personvernkonsekvensane vurderte av lovgivaren, og det er gitt utfyllande reglar i lov og forskrift for å sikre personvernet til dei registrerte.

Det er likevel utfordringar knytte til å gi samtykke til behandling av personopplysningar til andre føremål enn det å få helse- og omsorgstenester. Relasjonen mellom lege og pasient blir sjeldan opplevd som likeverdig. Det er derfor viktig at pasienten ikkje blir sett i ein situasjon som inneber ei oppleving av at samtykke vil kunne få innverknad på relasjonen til helsepersonellet og den helsehjelpa som skal ytast.

Overfor pasienten kan det vere ei pedagogisk utfordring å skilje mellom helsepersonellet si rolle som utøvarar av helsehjelp og ei eventuell rolle som forskar. Det å gi eit reelt samtykke føreset ei oppleving av likeverd. Å leggje til rette for samtykke som grunnlag for bruk av personopplysningar i situasjonar der det finst ei binding mellom pasienten og behandlaren, kan vere ei etisk utfordring.

Reservasjonsrett mot behandling av helseopplysningar kan reelt sett innebere større valfridom og gi betre balanse mellom partane i enkelte samanhengar. Dette kan gi pasienten meir ro og tid til å vurdere eige standpunkt før det blir teke ei avgjerd. Behandlingsgrunnlag i lov eller i ein av dei nødvendiggjerande grunnane kombinert med ein reservasjonsrett for den registrerte kan dermed gi pasienten meir reell sjølvråderett og såleis eit betre personvern enn eit strengt krav om samtykke som behandlingsgrunnlag.

6.4.3 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. I mange samanhengar har mindreårige oppfatningar om behandling av personopplysningar om dei. Dei kan òg bli bedne om å bidra med opplysningar om seg sjølve, til dømes i forskingssamanheng eller ved medisinsk behandling. I nokre samanhengar kan mindreårige sjølve samtykkje i behandling av opplysningar, medan det i andre samanhengar er dei føresette som samtykkjer på vegner av den mindreårige. Somme gonger blir det kravd at begge partar gir samtykke til behandling av personopplysningar. På denne måten unngår ein at dei føresette samtykkjer i noko den mindreårige er sterkt ueinig i, eller omvendt. 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. Når føresette samtykkjer i at opplysningar om barnet kan behandlast, skal dei derfor alltid ha barnet sitt beste i tankane. Døme på behandlingar som sjeldan vil vere til barnet sitt beste, kan vere tilfelle der foreldre gjer informasjon om barn tilgjengeleg på nett i saker om barnevern eller barnefordeling.

Spørsmålet om samtykkekompetansen til mindreårige er særleg aktuelt ved behandling av personopplysningar i skule- og barnehagesektoren, i helse- og omsorgssektoren og i forskingssamanheng. I forskingssamanheng legg ein til grunn at samtykke frå føresette normalt er nødvendig når barn under 15 år skal delta i forsking. Det er likevel viktig å ta vare på sjølvråderetten til barnet. I tillegg til samtykke frå foreldra er barns eigen aksept derfor nødvendig frå dei er gamle nok til å gi uttrykk for at dei samtykkjer. I skule og barnehage legg ein òg vekt på barns rett til medverknad og prinsippet om at synspunkta til barna skal leggjast til grunn ut frå alder, føresetnader og mognad. Dette er direkte formulert eller kan tolkast ut frå relevant regelverk på området. Barnet sin rett til å bli rådspurt og sjølv få samtykkje i behandling av personopplysningar må derfor sjåast i lys av både prinsippet om barns rett til medverknad og kravet i personopplysningslova om at personopplysningar ikkje skal behandlast i strid med barnet sitt beste. I helsevesenet er samtykkekompetanse for mindreårige direkte regulert i helseregisterlova jamført med pasient- og brukarrettslova. Av dette regelverket følgjer klåre aldersgrenser for den mindreårige sin rett til å samtykkje i helsehjelp. 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. Likevel er det eit krav at dei samtykkjer i behandling av personopplysningar for at dei skal få tilgang til ulike tenester, til dømes når dei lastar ned applikasjonar og tenester til mobiltelefonane sine.

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 (for eksempel informasjonskapslar som blir lagra på maskina til brukaren og gir informasjon om rørsler på nettet). Barn og unge har ofte vanskeleg for å forstå samanhengen mellom nettaktiviteten og reklamen dei blir eksponerte for. Det kan vere vanskeleg å forklare dei samanhengen mellom «likes» på Facebook og reklamen i Facebook-profilen deira.

Samtykke til at personopplysningar kan nyttast til marknadsføring på nett, blir ofte gitt på lite tydelege måtar. Somme gonger ligg samtykke som ei førehandsinnstilling i tenesta, for eksempel i form av førehandsavkryssa boksar. Andre gonger blir det gitt samtykke til behandling av personopplysningar samtidig som ein takkar ja til sjølve tenesta. 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. Brukarane er yngre enn dei var for nokre år sidan, og bruken er langt meir omfattande enn då. Det er derfor grunn til å ha ein open diskusjon om kva mindreårige bør kunne samtykkje i sjølve, og når foreldre eller føresette bør gi samtykke på deira vegner.

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. Dette kan gjerast ved ulike tekniske løysingar, til dømes at samtykke skjer ved stadfesting via e-posten til føresette. Aldersgrensa på 13 år er vald mellom anna fordi dette er aldersgrensa i lovgivinga i USA[4].

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. Norske barn bruker tenester som blir tilbodne frå andre delar av verda. Ein kan neppe forvente at desse tenestetilbydarane vil tilpasse tenestene sine til eit særnorsk regelverk. Ein kan derimot forvente at dei tilpassar seg til vernenivået i resten av Europa. Samstundes må Noreg ha reglar som på ein god måte tryggjar barns personvern når dei bruker norske nettenester[5].

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. Noreg bør vere ein aktiv deltakar og bidragsytar i dette arbeidet, og på best mogleg vis påverke resultata av arbeidet til barna sitt beste. Både personvernstyremaktene og forbrukarstyremaktene kan spele viktige roller i dette arbeidet.

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[6]. Også frå anna hald, mellom anna Datatilsynet og Helsedirektoratet, har det vore etterlyst eit klårare regelverk om bruk av varslings- og lokalise-

---

4 COPPA: Childrens online privacy protection act.

5 Sjå mellom anna høyringsfråsegna frå Forbrukarombodet 12. juni 2012 til Justisdepartementet om EUs utkast til forordning om personvern, der dei gir uttrykk for at aldersgrensa for mindreårige sitt samtykke på nett må "setjast så høgt at barn som ikkje har føresetnad for å overskode konsekvensane av å gi samtykke, ikkje kan gjere det utan å involvere føresette".

6 NOU 2011: 11 Innovasjon i omsorg (kapittel 7.4.4)

ringsteknologi i tenesteytinga til pasientar og brukarar som manglar samtykkekompetanse.

Denne typen hjelpemiddel kan heve kvaliteten på tenestetilbodet og vere positive for pasientar og brukarar, særleg dei som lir av minnetap og demens. Det at pårørande eller helsepersonell kan bli varsla om potensielle farar eller kunne lokalisere personar som er forsvunne, kan bidra til at mange av desse menneska kan leve eit friare og meir normalt liv med meir fysisk aktivitet. Det kan òg bidra til at dei får høve til å bu heime lenger. Samstundes er det viktig at den nye teknologien ikkje erstattar mellommenneskeleg kontakt og sosialt samvær.

Det finst mange ulike teknologisk løysingar, og ein må konkret vurdere val av tiltak for og oppfølging av kvar einskild pasient eller brukar. Sjølv om varslings- og lokaliseringshjelpemiddel (til dømes GPS) kan gi pasientane og brukarane ei auka kjensle av integritet og sjølvstende, må ein òg vurdere tiltaket i eit personvernperspektiv. 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). Bruk av samtykke som grunnlag for behandling av personopplysningar er likevel vanskeleg i situasjonar der ein behandlar personar med til dømes demens. For at pasientane eller brukarane skal kunne gi samtykke etter lova, må dei vere i stand til å forstå kva bruken av personopplysningar inneber, det vil seie at dei 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.

6.4.4 Gir samtykke alltid godt personvern?

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.

Likevel er det 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[7] på oppdrag frå Moderniseringsdepartementet og Datatilsynet. Undersøkinga viste at nordmenn flest reflekterer lite over eige personvern. Mange er lite medvitne om korleis opplysningar om dei blir behandla. Berre ein liten del av befolkninga kjenner personvernrettane sine, og endå færre bruker dei rettane regelverket gir dei. Mange gir frå seg personopplysningar sjølv om dei eigentleg ikkje ønskjer å gjere det, til dømes på ulike nettenester. 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. Mange seier truleg ja til noko dei ikkje veit kva er. Det er grunn til å tru at dette skjer relativt ofte, og det er urovekkjande. Ikkje minst er det urovekkjande i samanhengar der det blir behandla mange og sensitive personopplysningar over eit langt tidsrom eller til uklåre føremål. Det er òg urovekkjande i samanhengar der innsamla informasjon skal vere tilgjengeleg for ei stor brukargruppe.

Verdien av samtykke som behandlingsgrunnlag har vore framheva og understreka dei siste åra, både nasjonalt og internasjonalt. Det blir lagt generelt stor vekt på at dei registrerte skal ha kontroll med behandling av opplysningar om seg sjølve. Informert samtykke står sentralt i denne samanhengen. 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. I nokre samanhengar kan ein spørje om bruk av samtykke som behandlingsgrunnlag nærmast fungerer som ei ansvarsfråskriving for den behandlingsansvarlege. Artikkel 29-gruppa i EU har drøfta dette i sin *Opinion 15/2011 on the definition of consent*. I oppsummeringa av dette dokumentet skriv arbeidsgruppa at dersom samtykke blir brukt feil, er det illusorisk, og samtykke blir eit utilstrekkeleg behandlingsgrunnlag.

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. Alle tek

[7] TØI-rapport 789/2005, Ravlum

meir eller mindre gode val på meir eller mindre godt grunnlag. Innbyggjarane bør ha same råderetten over behandling av personopplysningar som over andre forhold som direkte vedkjem dei, til dømes om dei vil forsikre eigedelane sine når dei skal på ferie. At personvernval av og til blir tekne på sviktande grunnlag, er derfor ikkje eit argument mot at samtykke skal vere eit tilrådd behandlingsgrunnlag.

6.5 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 annan 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. To svært ulike personopplysningsbehandlingar som begge bruker reservasjonsrett, er behandling av personopplysningar for bruk i direkte marknadsføring og behandling av personopplysningar i samband med etableringa av den nasjonale kjernejournalen som er nemnd ovanfor. Ingen av desse behandlingane kan rettsleg sett seiast å vere basert på samtykke, men har eit anna rettsleg grunnlag for behandling av personopplysningar. 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.

6.6 Samandrag og tilrådingar

I offentleg sektor vil behandling av personopplysningar normalt ha heimel i lov eller eventuelt vere ein nødvendig føresetnad for utøving av offentleg myndigheit. Som heimel reknar ein òg reglar som føreset at det blir behandla personopplysningar som er nødvendige for å oppfylle føremålet med lova. Samtykke bør likevel òg i framtida vere det føretrekte behandlingsgrunnlaget i samanhengar der dei registrerte har eit reelt val med omsyn til om dei vil la seg registrere. Samtykke som behandlingsgrunnlag i offentleg sektor skal berre brukast når grunnlaget for samtykke er reelt. Informasjon om og samtykke til behandling av personopplysningar gir dei registrerte godt grunnlag for å ta vare på sitt eige personvern. Samtykke gir råderett over behandling av eigne personopplysningar. Dette er

eit viktig personvernprinsipp, og det blir framheva stadig oftare i personvernsamanheng, både nasjonalt og internasjonalt.

Utgreiingar av personvernkonsekvensar i lovgivingsprosessen kan medverke til større merksemd på behovet for og innretninga på personopplysningsbehandlinga og dermed gi klårare lovheimlar for behandling av personopplysningar.

Samtykke frå mindreårige til behandling av personopplysningar reiser særlege utfordringar. Når føresette skal samtykkje i behandling av personopplysningar på vegner av barn, skal barnet sitt beste alltid leggjast til grunn. Også barnet si meining skal ha vekt.

Å gjere det mogleg for dei registrerte å reservere seg mot behandling av personopplysningar kan vere ei god personvernløysing der personopplysningsbehandlinga er lovleg, men der behandling av opplysningar om den enkelte ikkje er påkravd.

Boks 6.2 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.

7 Personvernrettar og -plikter

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. Rettane og pliktene som er nedfelte i personopplysningslova, speglar kvarandre. Dette inneber til dømes at når dei registrerte har innsynsrett, har den behandlingsansvarlege plikt til å gi informasjon.

Ein del personvernrettar er òg nedfelte i anna regelverk, og dette regelverket kan i praksis ha meir å seie enn personopplysningslova. Forvaltningslova[1] § 18 inneheld for eksempel ein vid rett for partane i ei sak til å gjere seg kjende med opplysningar i saka, likevel med dei avgrensingar som følgjer av forvaltningslova §§ 18 a –19. Innsyn i opplysningar om ein sjølv kan vere viktig for å kunne vurdere om ei sak blir behandla på riktig faktisk grunnlag. 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. Teiepliktsreglane skal hindre spreiing av opplysningar som dei registrerte ønskjer diskresjon om.

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.

7.1 Brukarmedverking og kontroll over eigne personopplysningar

Personvern er både ein kollektiv og ein individuell rett. Det vil seie at både samfunnet og den enkelte har interesse av å tryggje personvernet. For at ein skal kunne oppretthalde eit godt personvern for enkeltpersonar, er det viktig at den enkelte har ein viss grad av kontroll over eigne personopplysningar og reelt høve til å påverke korleis dei blir brukte. 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.

7.1.1 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. Sjølvråderetten kjem blant anna til uttrykk i reglane i personopplysningslova om samtykke som grunnlag for behandling av personopplysningar, som det er gjort greie for i kapittel 6.

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 er uløyseleg knytte til identifiserbare personar, og det er derfor viktig for dei å ha kontroll over opplysningane og bruken av dei.

Personopplysningar har i lang tid vore ei vare og samstundes eit betalingsmiddel. Mange gir frå seg personopplysningar i byte mot andre gode. Eit eksempel er kjøpshistorikk som blir registrert og lagra i tilknyting til bruk av ulike typar lojalitetskort i varehandelen. Dette kan gi tilgang til tilbod og tenester ein elles ikkje ville ha fått, eller som ein måtte ha betalt meir for i reine pengar. Dei færraste tenkjer over kor stor verdi personopplysningane om dei har for næringsdrivande. Viljen næringslivet har til å betale for personopplysningar, er likevel relativt liten, samstundes som verdien personopplysningar har for dei i kommersiell samanheng, synest høg. Med eit vell av tilsynelatande gratis tenester på nett og aktørar som tek betalt for tenestene sine i personopplysningar (som ulike sosiale medium og informasjonstenester), deler den enkelte ei stor mengd personopplysningar med desse aktørane for å kunne nytte

[1] Lov om behandlingsmåten i forvaltningssaker 10.02.1967

tenestene deira utan å betale med pengar. 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. Utan kunnskap om pågåande behandling av personopplysningar har dei registrerte lite grunnlag for å stille spørsmål og kan vanskeleg utøve kontroll. Retten til informasjon og retten til innsyn er derfor grunnleggjande i personvernsamanheng. Med grunnlag i informasjon om ei planlagd eller pågåande behandling av personopplysningar kan dei registrerte ta hand om både personvernrettar og andre rettar. Til dømes gir retten til innsyn i eigen pasientjournal høve til betre innsikt i eigne helseforhold og dei vurderingar behandlande helsepersonell har gjort.

Ivaretaking av retten til informasjon om behandling av personopplysningar vil bli diskutert nedanfor i kapittel 7.4.

7.1.2 Rett til anonymitet

I mange daglege gjeremål lèt innbyggjarane etter seg informasjon som gir høve til personidentifisering. Registrering i heilautomatiske bomstasjonar er eit eksempel på dette. Eit anna eksempel er avanserte måle- og styringssystem for energi, såkalla smarte målarar, som utan avbrot registrerer energiforbruket og rapporterer det til energileverandøren. Ulike automatiserte registrerings- og betalingssystem forenklar kvardagen både for tenesteytaren og -mottakaren. Automatiseringa held prisane nede og gjer tenestene meir tilgjengelege for brukarane. Personidentifiserbar informasjon frå registreringsordningane kan likevel, både åleine og saman med annan informasjon, seie mykje om rørslene og åtferda til dei registrerte.

Med omgrepet anonymitet forstår ein normalt at identiteten ikkje er kjend. Dersom ein tek utgangspunkt i at identitet er noko den enkelte sjølv har kontroll over, bør ein òg ha rett til å velje å vere anonym. 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, det vil seie at den behandlingsansvarlege ikkje skal behandle fleire opplysningar enn nødvendig for føremålet. Er identifikasjon ikkje nødvendig, skal dei registrerte ha høve til å opptre anonymt.

Boks 7.1 Frå St.meld. nr. 17 (2006-2007) tiltak 8.2

I St.meld. nr. 17 (2006-2007) skreiv regjeringa følgjande om tiltak for å sikre at det skal finnast tilbod om anonyme løysingar i samanhengar der det ikkje er nødvendig å identifisere seg:

> «Anonyme løysingar skal vere tilgjengelege i samanhengar der dette er føremålstenleg. Regjeringa vil greie ut moglegheita for
> – Pseudonyme løysingar som alternativ til full anonymitet og full identifikasjon.
> – Pseudonyme sertifikat i løysingar for digital signatur der dette er tilstrekkeleg.
> – Anonyme betalingskort som alternativ til bankkort/kredittkort som er knytte til identitet.»

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. Dette gjeld blant anna i samband med grensekontroll. Innreise til USA krev at den reisande gir betydelege mengder informasjon, samstundes som flyselskapa som flyr frå Europa til USA, pliktar å levere mange opplysningar om dei reisande til amerikanske styremakter. Dette er basert på dei såkalla PNR-avtalene[2] og skal blant anna hindre terrorisme. Auka terrorisme og illegal innvandring har medført vesentleg strengare grensekontroll det siste tiåret. Ved internasjonale reiser har den reisande derfor avgrensa høve til å reise anonymt.

Også i alminneleg varehandel er anonymiteten på vikande front. Stadig fleire innkjøp blir gjort

[2] Passenger Name Record, avtale mellom EU og USA av 8. desember 2011 om behandling og overføring av passasjerinformasjon til United States Department of Homeland Security (17434/11)

med betalingskort framfor kontantar. Utviklinga er ønskt både av styremaktene og næringslivet, blant anna fordi det er vesentleg innsparing knytt til korttransaksjonar framfor kontanttransaksjonar. Det er også ein fordel for kundane å sleppe å gå med mykje pengar i kontantar. Ein konsekvens av aukande kortbruk er registrering av detaljert kjøpsinformasjon på identitet i lang tid ut ifrå krava i bokføringsregelverket. I St.meld. nr. 17 (2006-2007) gav regjeringa uttrykk for at det var ønskjeleg å sjå på om det var mogleg å bruke anonyme betalingskort som alternativ til dei alminnelege betalingskorta. Høvet til å handle anonymt synest likevel i realiteten å ha vorte redusert dei seinaste åra.

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. Ikkje minst gjeld dette i samband med utvikling av nye betalingstenester, der ein ser at det blir mindre og mindre høve til kontant betaling. Dei elektroniske reisekorta i kollektivtrafikken er eit eksempel på eit område der retten til anonymitet er teken hand om på ein god måte. Bransjen og styremaktene har saman utvikla ein standard for anonyme elektroniske reisekort[3]. Dette kan danne mønster for andre.

7.1.3 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. Dette skal vere ein generell rett til å krevje sletting av opplysningar som blir behandla i strid med gjeldande reglar, og som ikkje lenger er nødvendige for innsamlingsføremålet, eller der den registrerte trekkjer tilbake det samtykket som er grunnlaget for behandlinga av personopplysningar. Retten til å bli gløymd vil særleg kunne gi grunn til sletting av opplysningar som er lagde ut på nett.

Retten til å bli gløymd er ein god personverntanke. Dei fleste har på eit eller anna tidspunkt gitt frå seg personopplysningar som dei seinare ønskjer å få sletta, for eksempel fordi opplysningane ikkje lenger er nødvendige for det føremålet dei opphavleg skulle brukast til. Mange ønskjer òg å få sletta personopplysningar som er publiserte 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.

Eit viktig element i regelverksrevisjonen i EU er å gi den enkelte betre høve til å ta vare på sitt eige personvern. Ein rett til å bli gløymd skal medverke til å gi betre kontroll over den digitale delen av livet vårt – ein del som får stadig større omfang. 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. Frå forskingshald er det dessutan peikt på at ein omfattande rett til å bli gløymd kan vere svært vanskeleg å sameine med ivaretaking av det grunnleggjande forskingsetiske prinsippet om at det skal vere mogleg å dokumentere og etterprøve forskingsresultat.

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. Det synest ikkje urimeleg at dei som ikkje lenger ønskjer å ha ein profil på Facebook, skal kunne få utlevert eller sletta den informasjonen dei sjølve har lagt ut på profilen sin. Dette verkar heller ikkje spesielt problematisk med tanke på ytringsfridomen, sidan det i det alt vesentlege er ytringar den enkelte har sett fram om seg sjølv.

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

[3] http://www.datatilsynet.no/global/04_veiledere/bransjenormer/bransjenorm_e-billettering_endelig_01.pdf

vurderingstema. Eit spørsmål er òg kva opplysningar det er praktisk mogleg å få sletta. Ei plikt til å fjerne den informasjonen ein sjølv har publisert, er neppe korkje praktisk eller teknisk spesielt vanskeleg. Men når informasjon lovleg er lagd på nett, blir han spreidd raskt. Å få fjerna informasjonen på alle dei stader han kan tenkjast å ha hamna, kan vere vanskeleg. Det er derfor ein viss fare for at ein svært vidfemnande rett til å bli gløymd blir eit ideal utan reelt innhald.

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.

7.2 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. Desse pliktene blir i hovudsaka avspegla i rettane til dei registrerte. 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. Dei fleste behandlingsansvarlege har ikkje behandling av personopplysningar som hovudoppgåve. Behandlinga er ein konsekvens av den verksemda som blir driven. Etterleving av personvernregelverket kan vere krevjande for mange som i det daglege ikkje har merksemd retta mot behandling av personopplysningar.

Det er ei generell utfordring at personvernregelverket er lite kjent blant dei som behandlar personopplysningar. Undersøkinga som Trafikkøkonomisk institutt (TØI) gjorde av behandlinga av personopplysningar i norske verksemder i 2005[4], viste at så mange som 31 prosent av dei spurde hadde lite kjennskap til personopplysningslova, medan 51 prosent korkje hadde god eller dårleg kjennskap til regelverket. Særleg synest reglane om informasjonstryggleik, som er sentrale reglar i personvernsamanheng, å vere lite kjende. Når det gjaldt reglane om internkontroll og informasjonstryggleik, viste tal frå TØI-undersøkinga at både kjennskapen til og forståinga for behovet for regeletterleving var svak. Om lag 33 prosent av dei spurde sa at det ikkje var aktuelt for dei å ha ei systematisk oversikt over kva opplysningar som vart behandla i verksemda, og 13 prosent svara at det ikkje var aktuelt å ha rutinar for sletting av unødvendige opplysningar. Dette trass i at begge delar er nødvendige for å etterleve reglane i personopplysningslova. 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 tilsvarande TØI si frå 2005 for å få oppdatert informasjon om effekten av dei tiltaka som er gjennomførte for å auke kunnskapen om personvernregelverket dei seinare åra. Slik informasjon kan òg vere nyttig som grunnlag for den komande revisjonen av personopplysningslova.

Trygginga av personvernrettane er nært knytt til pliktene den behandlingsansvarlege har, og korleis vedkomande oppfyller dei. Til liks med reglane som heimlar rettane til dei registrerte, er òg reglane som viser kva plikter den behandlingsansvarlege har, 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.

7.3 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. Dette er òg eit nødvendig ledd i vurderinga av om ei førestående behandling av personopplysningar vil vere i samsvar med regelverket eller ikkje. Det er til dømes eit krav etter personopplysningslova at behandling av personopplysningar skal vere eigna til å oppnå det planlagde føremålet. For å kunne dokumentere at ei behandling er føremålstenleg, er det nødvendig å vurdere konsekvensane av behandlinga. Det gjeld òg eit krav om at den behandlingsansvarlege skal velje det tilta-

[4] TØI-rapport 800/2005, https://www.toi.no/getfile.php/Publikasjoner/T%d8I%20rapporter/2005/800-2005/T%d8I-rapport-800-2005.pdf

ket som er minst inngripande overfor den enkelte, samstundes som det er eigna til å oppnå føremålet. For å kunne dokumentere forholdsmessigheit, må ein vurdere alternative tiltak som kan vere eigna til å nå målet.

Ein analyse av personvernkonsekvensar kan vise at det er fleire konkurrerande eller motstridande personvernomsyn å ta hand om i ei sak. For eksempel kan interessa i at opplysningane skal vere fullstendige, stå i motstrid til interessa i diskresjon. Då må ein vurdere kva personverninteresse som skal vege tyngst. Ein kan blant anna ta ugangspunkt i kva interesser ein trur den registrerte sjølv vil vere mest oppteken av å ta vare på i den konkrete samanhengen. I utgangspunktet er det ikkje relevant å leggje vekt på kva omsyn det er enklast for den behandlingsansvarlege å ta hand om. I staden kan ein leggje vekt på kva interesse ein trur dei registrerte sjølve vil vere mest opptekne av å tryggje. Analyse av personvernkonsekvensar vil òg kunne vise at personvernomsyn står mot andre samfunnsomsyn eller private omsyn. Dette er nærmare omtala i kapittel 4 om proporsjonalitet og avveging av ulike interesser.

Ofte er det føremålet ein ønskjer å oppnå, så viktig både for samfunnet som heilskap og for den enkelte at ein er villig til å akseptere inngrep i personvernet. I slike samanhengar skal den behandlingsansvarlege setje i verk tiltak for å tryggje personvernet til dei registrerte på best mogleg måte. 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. Personvernfremjande bruk av teknologi og innebygd personvern er relevant i denne samanhengen. Desse temaa blir omtala nærmare i kapittel 9.2 om IKT.

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 administrasjonsdepartementet 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 når dei vurderer personvernkonsekvensar, blant anna korleis informasjon om rettleiinga kan integrerast i ulike opplæringsprogram i offentleg sektor.

Personvernvurderingane og konsekvensanalysane som skal gjennomførast før ei personopplysningsbehandling blir sett i verk, er dei same uansett om personopplysningar blir behandla i privat eller offentleg sektor. 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». Tanken er at den behandlingsansvarlege skal ha ei regelfesta plikt til å greie ut personvernkonsekvensar dersom nokon del av behandlinga kan representere eit særleg trugsmål mot personvernet til dei registrerte.

Personvernanalysar medverkar til å bevisstgjere dei behandlingsansvarlege om dei personvernutfordringane som ligg i eit planlagt tiltak. Analyseprosessen kan gi grunnlag for å vurdere alternative tiltak. Analysane vil truleg òg bidra til at personvernutfordringar kan bli tekne hand om rimelegare og betre enn om tiltaka kjem inn seint i planleggingsprosessen. Utgreiing av personvernkonsekvensar og gjennomføring av personvernanalysar bør derfor 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.

7.4 Plikt til å gi informasjon om behandling av personopplysningar

Det er ei prioritert oppgåve for styremaktene at innbyggjarane skal kjenne rettane sine og vere i stand til å ta hand om sitt eige personvern. For å oppnå dette er informasjon og kunnskap om behandling av personopplysningar avgjerande. Reglar om rett til informasjon om behandling av

opplysningar og om innsynsrett for dei registrerte, både i personopplysningslova og i spesialregelverk, skal ta hand om informasjonsbehovet. Terskelen for å oppsøkje informasjon kan vere høg. I mange samanhengar er det derfor ikkje tilstrekkeleg at den enkelte har rett til informasjon når vedkomande vender seg til den behandlingsansvarlege. I tillegg til å gi informasjon ved konkrete førespurnader har den behandlingsansvarlege derfor òg ei plikt til å gi ein del informasjon av eige tiltak.

7.4.1 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 måte som set den registrerte i stand til å ta hand om interessene sine. I det ligg det at informasjonen må vere klår og tydeleg.

For tre spesielle typar personopplysningsbehandlingar er det særskilde informasjonsreglar. Dette gjeld ved bruk av personprofilar, ved automatiserte avgjerder og i kredittopplysningsverksemd.

Ein personprofil seier noko om kva behov, preferansar og liknande ein person har, basert på ei samanstilling av informasjon om vedkomande eller om personar som liknar vedkomande. Slike profilar er det vanleg å nytte blant anna til marknadsføring. Ved bruk av personprofilar pliktar behandlingsansvarlege i Noreg å gi informasjon om kva opplysningstypar som er med i profilen, og kvar desse opplysningane er henta frå. Informasjonen er nyttig for å forstå korleis den behandlingsansvarlege har kome fram til den aktuelle profilen. Bruk av slike personprofilar er truleg langt meir utbreidd enn ein skulle vente ut frå informasjon om profilane til dei registrerte. Den norske regelen har ingen parallell i EUs personverndirektiv, og det inneber at behandlingsansvarlege som er etablerte i andre land, ikkje har tilsvarande informasjonsplikt når dei lagar profilar om norske brukarar av utanlandske tenester. Marknadsføring frå utanlandske tenestetilbydarar kan derfor vere basert på personprofilar utan at den registrerte har krav på informasjon om det.

Dersom det blir nytta automatiserte prosessar for å behandle personopplysningar og ta avgjerder med rettslege konsekvensar for den registrerte, gir personopplysningslova ein rett til å få ei forklaring av regelinnhaldet i programma som ligg til grunn for avgjerda. I praksis inneber dette at den registrerte kan krevje ei forklaring på korleis avgjerdstakaren er komen fram til resultatet. I offentleg forvaltning følgjer ei tilnærma lik grunngivingsplikt av forvaltningslova. Grunngivingsplikta i personopplysningslova er derfor mest relevant for privat sektor. Eit eksempel på ein type automatisert avgjerd som kan falle inn under informasjonsplikta, er avslag på kredittsøknader som er gitt på bakgrunn av ein fullstendig automatisert scoremodell. Ein del kredittytarar, særleg ved kredittsal i nettbutikkar, baserer seg kun på slike automatiserte kredittvurderingar. Retten til å få ei utgreiing om regelinnhaldet i datamaskinprogrammet kan for eksempel ha verdi for registrerte som vurderer å klage på ei slik automatisert avgjerd.

Den tredje typen behandling av personopplysningar som det finst særlege informasjonsreglar for, er behandling av opplysningar i kredittopplysningsverksemd. Mange opplever utlevering av kredittopplysningar som integritetskrenkjande. For at dei registrerte skal vere informerte om kva opplysningar kredittopplysningsbyråa har om dei, er byråa pålagde å varsle dei registrerte både ved innsamling av enkelte opplysningstypar som gjeld kredittvurderinga, og ved utlevering av opplysningar. Varsel ved innsamling gir den registrerte høve til å reagere dersom han eller ho meiner det er registrert ukorrekte opplysningar. Opplysningsplikt ved utlevering gir viktig informasjon om kven som tek imot og behandlar kredittopplysningar om ein sjølv. Den som ber om å få utlevert kredittopplysningar, veit samstundes at den omspurde vil få kopi av opplysningane. Dette kan motverke uthenting av opplysningar utan sakleg behov. Gjenpartsplikt har vore praktisert i kredittopplysningsverksemd i mange år og synest å fungere godt.

7.4.2 Etterleving av informasjonsreglane

For å setje innbyggjarane betre i stand til å ta hand om sitt eige personvern, er det 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. Generell informasjon om ei personopplysningsbehandling som skal vere tilgjengeleg for alle, er informasjon som med fordel kan liggje tilgjengeleg på nettsidene til ei verksemd. Dette er grunnleggjande informasjon om behandling av personopplysningar som i dei fleste tilfelle ikkje treng hyppig oppdatering. På nettsidene til Datatilsynet finn ein denne typen informasjon under overskrifta personvernerklæring[5]. Der finn brukarane informasjon om kva opplysningar som blir samla inn og behandla ved bruk av dei ulike tenestene på sidene, og dessutan om kven som er behandlingsansvarleg og databehandlar. Både offentlege og private behandlingsansvarlege bør sørgje for å ha slik informasjon lett tilgjengeleg på nettsidene sine, for eksempel under overskrifta *personverninformasjon* eller *personvernerklæring*. Dessutan bør informasjonen vere i eit format som gjer at han lett kan sendast til dei som ønskjer informasjon på andre måtar enn via nettet. For å hjelpe dei behandlingsansvarlege til å oppfylle informasjonspliktene sine vil regjeringa utarbeide ein mal for denne typen informasjon.

Døgnopen forvaltning er eit aktuelt tema. Dei fleste har vorte vande med å ha tilgang til ei rekkje tenester på nett heile døgnet. Nettbaserte tenester er praktiske og brukarvenlege for innbyggjarane, samstundes som dei er ressurssparande og effektive for tenesteytaren – anten det er offentlege eller private tenester ein ønskjer tilgang til. 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. Ønskjer den registrerte innsyn i opplysningar om seg sjølv, kan han eller ho få det gjennom ulike sikre løysingar for innlogging. Gjennom *Digitaliseringsprogrammet* har regjeringa gitt uttrykk for at det er eit mål at mest mogleg av kommunikasjonen mellom innbyggjarane og forvaltninga skal skje elektronisk. Dette er både rimeleg, miljøvenleg og praktisk. System som skal behandle personopplysningar, bør derfor leggje til rette for elektronisk kommunikasjon med dei registrerte i den grad dette går saman med nødvendig tryggleik i systemet.

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. Både innan bank og forsikring og hos tilbydarar av elektronisk kommunikasjon finst det gode eksempel på personverninformasjon på nett og elektroniske innsynsløysingar. Store offentlege etatar som NAV, Statens lånekasse, Statens pensjonskasse og skatteetaten har innloggingsløysingar der brukarane kan få tilgang til ein del informasjon om seg sjølve i tillegg til ei rekkje tenester frå etatane. 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. Slik gjenpartsplikt gir dei registrerte automatisk verdifull informasjon om bruken av opplysningar om dei. I Innst. 348 L (2011–2012) frå Helse- og omsorgskomiteen om oppretting av nasjonal kjernejournal rår komiteen til at den enkelte på sikt bør få høve til å bli automatisk varsla dersom helsepersonell opnar kjernejournalen til vedkomande. Komiteen meiner dette er ei praktisk og føremålstenleg oppfølging av kravet om at pasientane skal ha rett til innsyn i loggen over opningar av eigen kjernejournal. Regjeringa legg til grunn at elektronisk gjenpartsplikt kan vere ein praktisk måte å gjennomføre innsynsrett på i mange samanhengar. Særleg er det eit godt verkemiddel der personopplysningar er tilgjengelege for svært mange brukarar, som i helsesektoren, i arbeids- og velferdsforvaltninga og i bank- og finansnæringa. Samstundes må ein ikkje bruke ordninga på ein måte som medfører at dei registrerte druknar i informasjon. Blir det for mykje informasjon, blir han ikkje lesen, og ordninga kan miste verdien sin. 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

[5] http://datatilsynet.no/Om-Datatilsynet/Datatilsynets-nettsider/

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 er viktig at undervisningssektoren gir elevar i ungdomsskulen og den vidaregåande skulen god og forståeleg informasjon om behandlinga av personopplysningar om dei, blant anna i tilknyting til bruk av digitale læringsplattformer i skulen. Det finst allereie informasjon på området utarbeidd av Senter for IKT i utdanninga. Dette materiellet bør skuleeigaren nytte som ledd i opplæringa og bevisstgjeringa av elevane.

7.4.3 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. Dette inneber at ein må gi informasjonen på ein måte som gjer han forståeleg, og at det er mogleg å ta stilling til han.

Det har den seinare tida vore større merksemd om dei tallause, omfattande og kompliserte personvernerklæringane som finst på nettet. Mange av desse erklæringane er svært juridiske i forma. Dette fører igjen til at dei er vanskelege for lesarane å forstå. Lesarvenlege og forståelege personvernerklæringar kan derfor vere eit viktig bidrag til å gi dei registrerte betre høve til å ta hand om eige personvern.

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.

7.5 Lagringstid

7.5.1 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. I politiregisterlova § 50 heiter det til dømes at opplysningar «skal ikkje lagrast lenger enn det som er nødvendig for formålet med behandlinga». Andre lovreglar har derimot heilt konkrete slettereglar, og dei vil gå føre dei generelle slettereglane i personopplysningslova. Eit døme på ein slik sletteregel finst i lov om elektronisk kommunikasjon § 2-7 a første leddet, der det heiter at opplysningar frå elektronisk kommunikasjon kan lagrast i seks månader for gitte føremål. Det ligg implisitt i dette at etter seks månader finst det ikkje lenger sakleg behov for opplysningane, og då skal dei slettast.

7.5.2 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 er billig og enkelt å ta vare på informasjon som blir generert i ulike IKT-system. Dette gjeld både primærinformasjon, det vil seie den informasjonen brukaren bevisst utarbeider, og sekundærinformasjon, det vil seie informasjon om kva brukaren har gjort når han eller ho har brukt systema for å generere primærinformasjon. Eit eksempel på sekundærinformasjon er loggar i datasystem, der all informasjon om bruken av systema ligg. Enorme mengder informasjon krev liten lagringskapasitet samanlikna med tidlegare. 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. Det er for eksempel mogleg å datomerkje informasjon med utløpsdato som indikerer at ein bør kontrollere kvaliteten og relevansen til opplysningane. Dette kan gjerast ved ei teknisk løysing som varslar den behandlingsansvarlege når personopplysningar ikkje har vore nytta eller ikkje har vorte oppdaterte på ei stund. Dersom det er juridisk mogleg, kan ein implementere automatiserte sletterutinar. I offentleg sektor vil arkivregelverket setje grenser for høvet til å slette opplysningar. Eit alternativ til sletting i offentleg sektor kan vere varsel om at ein bør vurdere å overføre opplysningane til arkiv. Eventuelle automatiserte rutinar i det offentlege må ta omsyn til fristane i arkivregelverket. Automatiserte rutinar vil sørgje for at opplysningar ikkje blir lagra i lang tid utan å bli brukte, eller utan at det blir vurdert om dei er relevante for innsamlingsføremålet. Tilrettelegging av slike system gir òg ei oppfordring til den behandlingsansvarlege om å tenkje gjennom og ta aktiv stilling til sletterutinar.

Skal automatiserte slette- og arkiveringsrutinar fungere, krevst det grundige vurderingar når dei blir etablerte. Ein må gjennomføre nøkterne vurderingar av kva som er føremålstenleg lagringstid for ulike opplysningstypar. Ein må òg få på det reine om det eksisterer lagringsplikter som gjer sletting umogleg. Sannsynlegvis må ulike typar opplysningar som er med i same behandlinga, ha ulike lagringstider og slettefristar. 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.

7.6 Internkontroll

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, sjølv om ein med fordel kan følgje systematikken på tryggleiksområdet. 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. Dette er i tråd med resultata frå TØIs personvernundersøking blant norske verksemder i 2005[6]. 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. Slike ombod fungerer som personvernrådgivarar i verksemdene sine og kan bidra til at leiinga legg større vekt på å få utarbeidd og dokumentert rutinar og system som skal ta hand om personvernet.

Datatilsynet har utarbeidd omfattande kunnskaps- og rettleiingsmateriell, medrekna opplæringsprogram om internkontroll og informasjonstryggleik som blant anna er tilgjengelege på nettsidene til etaten. Det er viktig å spreie kunnskap og informasjon om dette materiellet til relevante brukargrupper.

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. Dette vil vere eit supplement til den generelle dokumentasjonen Datatilsynet har utarbeidd, men vil vere særleg retta mot internkontroll i offentleg verksemd. Rettleiingsmateriell som er særleg retta mot offentleg sektor, vil vere eit viktig bidrag til å leggje til rette for ei heilskapleg tenking omkring ivaretaking av personvern.

---

[6] TØI-rapport 800/2005

Boks 7.2 Tema for rettleiinga om internkontroll på personvernområdet i offentleg verksemd

- Identifisering av behandlingar, føremål, rettsleg grunnlag, ansvar og plikter som følgjer av behandlinga
- Informasjon om det daglege ansvaret for dei ulike delane av behandlinga
- Rutinar for sjølvstendig oppdatering/sletting av personopplysningar
- Rutinar for behandling av krav om retting/sletting
- Rutinar for behandling av krav om innsyn
- Informasjonsplikt
- Rutinar for etterleving av krav til informasjonstryggleik
- Rutinar for etterleving av melde- og konsesjonsreglane
- Oppfølging av om internkontrollen blir etterlevd, om han er kjend, og om han er tilstrekkeleg
- Avvikshandtering, rapportering til tilsynsstyremakter

7.6.1 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. Logging av oppslag i system, som omtala i kapittel 9.6, kan vere eit godt verkemiddel. Ved å ha gode, dokumenterte og kjende rutinar for avvikshandtering kan ein redusere eventuelle skadar ved avviket. Ikkje minst vil ei rask rapportering til Datatilsynet setje tilsynet i stand til å gi råd og rettleiing om korleis ein kan redusere skadepotensialet, og korleis ein kan unngå liknande hendingar i framtida.

Ei rekkje tryggleiksbrot blir aldri rapporterte til Datatilsynet. Mangel på kunnskap om regelverket kan vere ei årsak til manglande avviksrapportering. Låge rapporteringstal kan òg kome av at dei behandlingsansvarlege vegrar seg for å rapportere avvik fordi dei fryktar negativ omtale dersom saka blir kjend. Dei negative konsekvensane kan likevel bli meir alvorlege om ein lèt vere å handtere avvik på ein god måte. Å ta ansvar for feil vil i dei fleste tilfelle verke meir tillitvekkjande enn det motsette. 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.

7.7 Samandrag og tilrådingar

Personvern handlar for ein stor del om informasjon. Det er eit uttala mål at innbyggjarane i størst mogleg grad skal ha råderett over sine eigne personopplysningar og vere i stand til å ta hand om sitt eige personvern. Dei registrerte har rett til å få informasjon om behandlinga av personopplysningar om dei og kva som er føremålet med behandlinga. Dei skal òg vite kva rettar dei har i samband med personopplysningsbehandlinga.

Regjeringa arbeider for å digitalisere offentleg sektor. I dette arbeidet vil auka tilgjengeleggjering av personopplysningar i elektroniske innsynsløysingar kunne vere aktuelt.

Det er den behandlingsansvarlege som har ansvaret for at dei registrerte får nødvendig informasjon på ein forståeleg måte. For å hjelpe dei behandlingsansvarlege til å oppfylle informasjonspliktene etter personopplysningslova vil regjeringa få utarbeidd ein mal for denne typen informasjon.

Elektronisk gjenpart kan vere ei god løysing for å gi informasjon til dei registrerte, samstundes som det kan bevisstgjere dei behandlingsansvarlege. Det offentlege bør vurdere bruk av slike løysingar når nye register blir planlagde og nye IKT-system innkjøpte.

Dataminimalitet er eit godt personvernprinsipp, og det bør leggast til rette for bruk av sporfrie alternativ der dette er praktisk mogleg. Ein bør vurdere bruk av teknologi som kan redusere mengda av overskotsinformasjon. Eit anna tiltak for å avgrense mengda av personopplysningar kan

vere å leggje til rette for automatiserte arkiverings- eller sletterutinar når ein utviklar nye IKT-system der regelverket ikkje er til hinder for slike løysingar.

For å få klårare fram kor viktig det er å greie ut personvernkonsekvensar, vil regjeringa arbeide for at saksbehandlarar i offentleg sektor skal kjenne og bruke den eksisterande rettleiinga når dei vurderer personvernkonsekvensar. Informasjon om rettleiinga vil bli integrert i ulike opplæringsprogram i offentleg sektor. Det vil òg bli lagt til rette for at informasjon om plikta til å gjennomføre personvernanalysar kan distribuerast saman med annan informasjon som blir gitt til næringsdrivande når dei startar næringsverksemd.

God internkontroll er som oftast eit resultat av bevisste personvernval i verksemda. Regjeringa vil leggje til rette særskilt rettleiingsmateriell for å gjere det enklare å etterleve internkontrollplikta på personvernområdet i offentleg sektor.

Boks 7.3 Hovudpunkt kapittel 7

- 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.

8 Sosiale medium og personvern

8.1 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.

Eit kjenneteikn ved sosiale medium er at kvar einskild brukar fritt kan publisere informasjon som blir gjord tilgjengeleg for ein vid krins, utan at det som blir publisert, går gjennom nokon kvalifisert førehandskontroll av ein redaktør. Slik informasjonsspreiing kan skape personvernutfordringar, for eksempel ved publisering av bilete av personar som ikkje har gitt samtykke, eller når bilete og tekst blir sett inn i ein samanheng som er misvisande eller belastande. Sosiale medium som Facebook, Twitter og YouTube er i bruk over heile verda. Det inneber at spreiinga av informasjon via desse media potensielt er global. For å kunne ta del i sosiale medium gir brukarane frå seg personopplysningar. Det gjer 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. Slik kan det enorme sosiale nettverket òg seiast å ha utvikla det største, og kanskje òg mest intrikate, lageret av personopplysningar – alt på den korte tida dei har eksistert sidan 2004. Facebook har fått omtale i kapittel 8.6, men det finst uendeleg mange andre sosiale nettverk som nordmenn bruker dagleg, både norske og utanlandske.

Barn og unge er hyppige brukarar av sosiale medium. Ei «trygg bruk»-undersøking frå Medietilsynet frå 2010[1] *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. Medianalderen for debut på internett fell og var i 2010 mellom fem og seks år. Før fylte sju år hadde 37 prosent vore på internett, og hos barn mellom 9 og 16 år hadde 57 prosent besøkt eit nettsamfunn i løpet av ei veke. I ei undersøking frå 2012 *Småbarn og medier*[2] kjem det fram at 10 prosent av barna frå fem til åtte år og 33 prosent av barna frå ni til tolv år bruker internett dagleg. Undersøkinga viser òg at foreldra til dei yngste barna (fem–åtte år) hovudsakleg uroar seg for at barnet skal dele personlege opplysningar på internett, medan foreldra til dei eldre barna (ni–tolv år) uroar seg mest for at nokon skal publisere uheldige/upassande bilete av barna på internett.

Barn har fått eit særskilt internasjonalt vern gjennom FNs barnekonvensjon artikkel 16. Barn og unge er avhengige av andre for å kunne ta hand om eigne rettar. Dei som forvaltar interessene til barn og unge, for eksempel gjennom å gi samtykke på deira vegner, skal handle til barna sitt beste og ikkje for å eksponere seg sjølve eller fremje sine eigne interesser.

8.2 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

[1] http://www.medietilsynet.no/Documents/Trygg%20bruk/Rapporter/Barn%20og%20digitale%20medier/100319_Del_1.pdf

[2] http://www.medietilsynet.no/PageFiles/11282/120917_Rapport_smabarn_web.pdf

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. Det er først og fremst utviklinga av brukargenererte, elektroniske «medium» som har skapt nye utfordringar for personvernet. Dette er stadfesta av utgreiinga frå Medieansvarsutvalet, som konkluderte med at pressa si sjølvdømmeordning fungerer godt, og at det derfor ikkje er grunnlag for å etablere eit medieombod eller liknande.

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

8.3 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. Dette kan medføre ei samanblanding mellom det private og det offentlege, der grensene blir utviska. Samstundes kan publisering av informasjon skape personvernutfordringar, for eksempel ved publisering av bilete av ein person som ikkje har gitt samtykke, eller når eit bilete og tekst blir sett inn i ein samanheng som er misvisande eller belastande.

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. Det er jamleg fokus på tilfelle der barn på ein aller annan måte har vorte krenkte som følgje av misbruk av personopplysningar. Det kan for eksempel vere sjikane i form av mobbing eller publisering av bilete eller ved at tilgjengeleg informasjon blir sett inn i feil kontekst. 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. Ein SINTEF-studie frå 2009[3] viser at 36 prosent meiner det er utrygt å dele personleg innhald i dei sosiale media dei bruker mest. Få veit sikkert kven dei deler informasjon med når dei deler innhaldet på Facebook. Vidare opplyser brukarane at dei har lite oversikt over kva som skjer med innhaldet i det dei deler, og at dei er usikre på kva delar av profilen deira som er synlege for kven. I tillegg er det klåre utfordringar knytte til omfanget av deling av det innhaldet som blir publisert. SINTEF-studien viser at korkje unge eller vaksne i særleg grad klarer å verne sin eigen personinformasjon i sosiale medium.

8.4 Utanlandske tilbydarar av sosiale medium

Då sosiale medium for alvor byrja å breie om seg på midten av 2000-talet, var norske tenester blant dei mest populære i Noreg. VGs Nettby og Dagbladets Blink hadde åleine hundre tusenvis av brukarar kvar månad. No er begge desse tenestene nedlagde. 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. Ønskjer ein å blogge, er det i valet mellom blogg.no og Blogger.com irrelevant at den første tenesta er norsk og den andre amerikansk. Så lenge tenesta er føremålstenleg for brukaren, er det underordna kvar i verda tenestetilbydaren held til, eller kvar sjølve databehandlinga går føre seg. 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. Ein konsekvens av dette er at sosiale medium som rettar seg mot nordmenn, først og fremst held seg til lovverket i det landet der tenesta er etablert. Ein norsk brukar av Blogger.com vil i utgangspunktet ikkje nødvendigvis kunne få fjerna eit bilete som er

[3] Petter Bae Brandtzæg og Marika Lüders (2009): *Privat 2.0: Person- og forbrukarvern i den nye mediaverkelegheita.* Oslo: Sintef IKT.

publisert utan samtykke, slik norsk lovgiving gir han eller henne rett til. Dette kjem av at Blogger held seg til amerikansk og ikkje norsk rett.

8.5 Generelle personvernutfordringar ved bruk av sosiale medium

Internett har revolusjonert måten innbyggjarane kommuniserer på. Frå å vere ein stad der ein først og fremst tek imot informasjon, har nettet utvikla seg til å bli ein stad der ein òg aktivt deler og spreier informasjon. Denne utviklinga har utan tvil hatt ein demokratiserande effekt, men ho har òg gitt nye, store utfordringar for personvernet.

8.5.1 Openheit og transparens

Å delta i sosiale medium involverer behandling av store mengder personopplysningar. Bruce Schneier, forfattar og tryggleikssekspert, skil mellom ulike kategoriar av opplysningar som sosiale medium registrerer og lagrar om brukarane sine.[4] Sjølv om detaljane i kategoriseringa kan diskuterast og problematiserast, er lista i boks 8.1 meint som ein illustrasjon på breidda i opplysningar som blir involverte ved bruk av sosiale medium.

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. Følgjande utdrag frå personvernvilkåra til Twitter (5. mars 2012)[5] er eit eksempel:

> «Vi engasjerer visse pålitelige tredjepartsleverandører til å utføre funksjoner og tilby tjenester for oss. Vi kan dele din personlige informasjon med disse leverandørene, men bare det som er strengt tatt nødvendig for å utføre disse funksjonene og tjenestene, og kun i samsvar med beskyttelse beskrevet under personvern.»

Twitter opplyser om at dei deler informasjon med «tredjepartsleverandører», men opplyser ikkje nærmare kven desse er. Dette gjer det umogleg for brukarane å gjere seg kjende med personvernpolicyane til tredjepartane. Dei kan i praksis ha mykje å seie for ivaretakinga av personvernet til brukarane.

Boks 8.1 Kategoriar av opplysningar i sosiale medium

- *Tenesteopplysningar («service data»):* Opplysningar som er obligatoriske for å ta i bruk tenesta (for eksempel e-postadresse og namn)
- *Publiserte opplysningar («disclosed data»):* Opplysningar ein sjølv publiserer, og som ein har kontroll over (for eksempel innlegg og bilete)
- *Fortrulege opplysningar («entrusted data»):* Opplysningar ein sjølv publiserer på sidene til andre brukarar, og som ein derfor ikkje har kontroll over (for eksempel kommentarar)
- *Uventa opplysningar («incidental data»):* Opplysningar som andre publiserer om deg (for eksempel kommentar eller bilete)
- *Åtferdsopplysningar («behavioral data»):* Opplysningar som tenesta samlar inn om kva du gjer og med kven (for eksempel tema du skriv om, eller lenkjer du trykkjer på)
- *Avleidde opplysningar («derived data»):* Opplysningar som tenesta trekkjer ut av andre opplysningar (for eksempel kan opplysningar om kva nyhendeartiklar ein les, seie noko om politiske preferansar)

8.5.2 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.

Mange får seg derfor ei overrasking når dei oppdagar at bilete dei ville dele med nokre utvalde vener, også er tilgjengelege via Google, eller at e-postkontoen blir fylt med reklame fordi e-postadressa har vorte seld til tenesta sine samarbeidspartnarar. Problemet som oppstår når brukarane aktivt må reservere seg mot søkjemotorindeksering eller mot deling av personopplysningar med tredjepartar, er at mange lèt vere å endre inn-

[4] http://www.schneier.com/blog/archives/2010/08/a_taxonomy_of_s_1.html (6.mars 2012)

[5] http://twitter.com/privacy (5.mars 2012)

stillingane på grunn av manglande informasjon eller kunnskap.

8.5.3 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. Auka omsetning av personopplysningar og digitale spor gjer at kommersielle aktørar i dag kan skreddarsy og målrette marknadsføring på personnivå med grunnlag i desse spora. Innsamling og kommersiell bruk av personopplysningar i digitale omgivnadar er i ferd med å bli ein forretningsmodell som i stor grad utfordrar personvernet. 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.

8.5.4 Sletting

I 2011 fekk *slettmeg.no* (sjå meir om denne tenesta nedanfor) over 6000 personlege førespurnadar. 23 prosent av dei gjaldt ønske om å slette ein profil eller konto frå nettet. 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. For eksempel blir filer knytte til ein konto hos blogg.no lagra på eksterne bilettenarar (t.d. bloggfiler.no), noko som fører til at bileta overlever profilslettinga.

8.6 Særleg om Facebook

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). Tenesta gjer det enkelt å opprette og oppretthalde sosiale kontaktar. Samstundes finn mange glede i å dele historier, bilete og anna med andre via Facebook-sida si.

Facebook har fått mykje merksemd i samband med måten dei behandlar personopplysningar på. I mai 2010 skulda Forbrukarrådet selskapet for å ha brote den norske personopplysningslova ved at dei gav tredjepartsapplikasjonar på Facebook løyve til å hente inn personopplysningar om brukarar som hadde lasta ned desse applikasjonane, og om venene deira som ikkje hadde lasta ned applikasjonane. I ein rapport frå Datatilsynet er det sett spørsmålsteikn ved om samtykket frå brukarane til behandling av personopplysningar, i alle fall for enkelte tenester, er gitt med tilbakeverkande kraft, altså ikkje gitt på førehand. Datatilsynet konkluderer med at det er ein generell mangel på transparens overfor brukarane når det gjeld korleis Facebook handterer personopplysningar.

Ein tilsynsrapport frå det irske datatilsynet om Facebook Ireland Ltd. har òg fått mykje merksemd. I tillegg til personvernutfordringane som Datatilsynet trekte fram i sin rapport, er det irske datatilsynet særleg uroa over graden av personvern i Facebooks rutinar når det gjeld å slette og/eller gi brukarane tilgang til alle opplysningar som er lagra i tilknyting til kontoane deira. Vidare er det irske datatilsynet uroa over utviklinga av den såkalla «friend finder»-funksjonen. Den bruker teknologi for andletsattkjenning til å kjenne att tidlegare «tagga» andlet i fotoalbuma til brukarane, slik at dei kan føreslå nye «tags». Kvar einskild medlem kan reservere seg mot at namnet hans eller hennar blir føreslått som ein «tag», men dette er ikkje ein del av dei førehandsdefinerte innstillingane, som godtek slik «tagging». Det dreiar seg altså om ein reservasjonsrett snarare enn eit aktivt samtykke.

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.

8.7 Ansvaret til den einskilde og det offentlege

Å delta i sosiale medium er frivillig. 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. Blant anna tilbyr det offentlege hjelp av ulike slag til menneske som opplever å bli krenkte på nettet. Det er i dag mange aktørar som informerer barn og unge om nettvett med stønad frå det offentlege. Både Medietilsynet, Post- og teletilsynet, NorSiS, Teknologirådet, Senter for IKT i utdanninga og Datatilsynet er i dag involverte i ulike former for arbeid med nettvett.

8.7.1 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. Prosjektet medverkar med ressursar på nett og gir råd til kommunar, skular og privatpersonar om barn og medium. «Tiltaksplanen for barn, unge og nye medier» blir utarbeidd av Medietilsynet på oppdrag frå dei fem departementa som er representerte i den interdepartementale arbeidsgruppa for trygg bruk av internett. Kulturdepartementet samordnar dette arbeidet.

8.7.2 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. På *Nettvett.no* får brukarane informasjon om blant anna bruk av e-post, chat og sosiale medium, spam, virus, deling av filer på internett, nettbank og vern mot angrep utanfrå. Tenesta femner vidare enn berre til bruk av sosiale medium og er meir teknisk innretta enn fleire av dei andre hjelpetenestene. *Nettvett.no* er laga av Post- og teletilsynet på oppdrag frå Samferdselsdepartementet, i samarbeid med andre styremakter, IKT-bransjen og representantar for brukarane.

8.7.3 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. Det er utarbeidd eitt undervisningsopplegg for ungdomssteget/vidaregåande (13–17-åringar) og eitt for dei eldste barna på barneskulen (9–13-åringar). Heile eller delar av undervisningsopplegget er teke i bruk i rundt 16 land i Europa og Nord-Amerika. Regjeringa har ytt betydelege midlar til utviklinga av undervisningsprogrammet.

8.7.4 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. Framlegget frå Datatilsynet førte til at det vart løyvd øyremerkte midlar frå budsjettet til Fornyings- og administrasjonsdepartementet, slik at tilsynet kunne setje i gang arbeidet med å byggje opp tenesta. *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. Dette kan vere materiale den enkelte har lagt ut sjølv og seinare ønskjer å få fjerna, eller materiale som er lagt ut av andre.

Datatilsynet hadde ansvar for drift av *slettmeg.no* i 2010 og 2011. I denne toårsperioden handterte tenesta godt over 9000 personlege førespurnader frå folk i alle aldrar. 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. Etter overføringa har talet på førespurnader auka til mellom 500 og 600 i månaden. Likeins har talet på treff på heimesida auka.

Det er utarbeidd statistikk for dei to første driftsåra til *slettmeg.no*. Statistikken viser at ein stor del av førespurnadene kjem frå ungdom mellom 16 og 25 år (28 prosent). Det er òg mange foreldre som har kontakta tenesta på vegner av barna sine.

I 2011 gjaldt den vanlegaste typen førespurnader sletting av eigen profil på nettet. Mange nettbrukarar opplever at måten ein kan slette ein brukarprofil eller ein konto på, er godt skjult, eller dei får beskjed frå tenestetilbydaren om at sletting ikkje er mogleg. I andre tilfelle er det vanskeleg å kome i kontakt med tenestetilbydaren. Mange av dei som kontakta *slettmeg.no* med denne typen problem, fekk god hjelp.

Ein grunn til å ønskje sletting av brukarprofil kan òg vere at nettenesta er nedlagd. Eit eksempel på dette er VGs *Nettby*, som vart nedlagd i desember 2010, men som då ikkje sletta brukarprofilar og innhald.

Uønskt biletpublisering på internett er eit stort problem i dag. 11 prosent av alle førespurnadene som kom til *slettmeg.no* i 2011, gjaldt bilete som nokon hadde lagt ut mot klagaren sin vilje. I nærmare halvparten av tilfella var den som hadde publisert det uønskte biletet, ein familiemedlem, ein ven/kjenning eller ein tidlegare partnar. Dette fortel at mange ikkje veit at det å publisere bilete på nettet som hovudregel krev eit frivillig, informert og uttrykkeleg samtykke frå den som er avbilda.

Som gjennomgangen over viser, blir det allereie gjort mykje godt førebyggjande arbeid. Arbeidet kan likevel verke noko fragmentert. 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.

8.8 Personvern og ytringsfridom på nett

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. Ytringsfridomen har fått vern i Grunnlova § 100, som vernar retten til å formidle opplysningar, informasjon og meiningar. Ytringsfridomen er vidare verna av Den europeiske menneskerettskonvensjonen (EMK) artikkel 10. På den andre sida er privatlivet verna av EMK artikkel 8, som òg set skrankar for behandling av personopplysningar. Reglane er inkorporerte i norsk rett gjennom menneskerettslova 21. mai 1999 nr. 30. Fleire av reglane i straffelova, medrekna straffelova § 390 om krenking av freden i privatlivet, § 390 a om omsynslaus åtferd og reglane om ærekrenkingar i §§ 246 og 247 kan òg avgrense ytringsfridomen.

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. Dette vart endra då Stortinget behandla og vedtok lovendringsframlegget i Prop. 47 L (2011–2012) i april 2012. Proposisjonen inneheld ei vurdering av personvern og ytringsfridom knytt til eit forslag om å fjerne unn-

Boks 8.2 VGs Nettby

Ei av problemstillingane knytte til personvern som gjer seg gjeldande i sosiale nettsamfunn, er spørsmålet om kva som skjer med personopplysningar som brukarane aldri slettar. Sletting kan vere vanskeleg å få til, eller brukaren gløymer å slette fordi han eller ho sluttar å bruke tenesta, eller fordi nettsamfunnet blir nedlagd. Då Nettby vart nedlagd, ønskte dei ansvarlege bak nettsamfunnet å ta vare på innhaldet til framtidig forsking. Datatilsynet sette seg imot dette fordi brukarane aldri hadde samtykt til slik vidare bruk av opplysningar. Vidare lagring var heller ikkje ei påreknelig følgje av å delta i nettsamfunnet. Saka vart avgjord av Personvernnemnda i oktober 2012, PVN 2012-03 Nettby[1].

Personvernnemnda slo fast at både dei dokumenta i Nettby som var heilt opne, og dei som var tilgjengelege for alle Nettby-medlemene, er omfatta av pliktavleveringsreglane til Nasjonalbiblioteket. Når dokumenta er overførte, skal VG slette Nettby-materialet. I Nasjonalbiblioteket vil materialet ikkje vere allment tilgjengeleg, men skal berre nyttast til forsking og dokumentasjon.

[1] http://personvernnemnda.no/vedtak/2012_03.htm

taket for «opinionsdannande» føremål frå personopplysningslova § 7. I vurderinga framhevar Justisdepartementet blant anna følgjande:

> «Nye teknologiske muligheter for å behandle personopplysninger aktualiserer behovet for klare regler og en entydig praksis om forholdet mellom ytringsfriheten og personvernet. Det er forutsatt i forarbeidene til § 7 at rekkevidden av kjernebegrepene i bestemmelsen må fastsettes i Datatilsynets praksis, jf. punkt 4.2 over. I likhet med utrederne mener departementet at loven gir Datatilsynet tilstrekkelig kompetanse til å prøve grensene etter § 7 som ledd i tilsynsarbeidet, og at Datatilsynet både kan og bør benytte denne kompetansen til å pålegge opphør av behandlinger som foretas i strid med bestemmelsen, jf. personopplysningsloven § 46. Dette vil typisk kunne være behandlinger av personopplysninger som ikke kan anses omfattet av unntaket i bestemmelsen, men som like fullt gjennomføres uten at personopplysningslovens krav er oppfylt. Et eksempel kan være nettsteder hvor offentlige ansatte henges ut med navn, bilde, stilling eller lignende, og hvor det er nokså klart at nettstedet neppe «utelukkende» bedriver virksomhet med journalistiske formål.
>
> Et illustrerende eksempel på de problemstillinger som § 7 ofte representerer er Personvernnemndas sak PVN-2010-11. Saken gjaldt en persons klage på Datatilsynets vedtak om sletting av informasjon om private beredskapshjem som var lagt ut på Internett. Den aktuelle nettsiden hadde blant annet et diskusjonsforum hvor konkrete barnevernssaker, herunder altså personopplysninger knyttet til et beredskapshjem, ble drøftet. Nemnda kom til at publiseringene var vernet av ytringsfriheten, slik at den som drev nettstedet altså ikke var omfattet av personopplysningsloven.
>
> Departementets lovforslag representerer et ønske om en viss endring i praksis i forhold til den avveining som nemnda foretok i den angitte sak. I den grad det er forenelig med Grunnloven § 100 og Norges konvensjonsforpliktelser bør hensynet til ytringsfriheten således tillegges noe mindre vekt i tilsvarende, fremtidige saker.
>
> Departementet understreker for ordens skyld at selv om loven med en slik kursendring skulle få anvendelse i noen flere situasjoner enn tidligere, vil likevel den enkelte bestemmelse i personopplysningsloven måtte tolkes i lys av ytringsfriheten.»

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.

8.9 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. Opplysningar på internett er det mogleg for alle å søkje opp. Det er enkelt å hente inn informasjonen frå heile verda. Informasjonen kan brukast til marknadsføring, vidaresal eller til andre framstøytar mot mindreårige. Slik bruk er ofte uønskt og i mange tilfelle ulovleg.

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. Informasjonen bør seie noko om kva som er føremålet med behandlinga/publiseringa, at det er frivillig å gi frå seg bilete/opplysningar, kor lenge opplysningane vil liggje på nettsida, kva konsekvensar og ulemper behandlinga/publiseringa kan ha, og eventuelt annan informasjon som er nødvendig for at dei føresette og den mindreårige skal kunne bruke rettane sine. 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.

8.10 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.

Ei av dei som tok kontakt med slettmeg.no, var ei mor som nettopp hadde mista sonen sin i ei ulykke. Sjølv om Facebook-kontoen hans ikkje var i bruk etter ulykka, dukka profilen likevel opp med jamne mellomrom under faner som «folk som har gebursdag i dag», «folk du kanskje kjenner» og liknande. Etter tallause forsøk på å slette profilen sjølv fekk ho til slutt hjelp av *slettmeg.no*.

Ein annan førespurnad til *slettmeg.no* gjaldt bilete av døde personar på nettstaden Youtube. Etter massakren på Utøya den 22. juli 2010 dukka det opp fleire mobilvideoar av døde ungdomar ved sjøkanten. Fleire av foreldra fortalde *slettmeg.no* at dei kjende igjen sine eigne søner og døtrer, og at dei opplevde det som svært belastande at filmane låg ute på nettet. Google, som eig Youtube, nekta likevel å fjerne filmane fordi dei korkje braut norsk lov eller Youtube sine eigne retningsliner.

For dei attlevande kan det by på utfordringar å spore opp og få tilgang til brukarprofilane til avdøde i ulike nettsamfunn. Det same kan gjelde høvet til å ha kontroll med opplysningar som tredjemenn kan kome til å publisere om den avdøde på nettet. Eksempla over viser 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.

8.11 Samandrag og tilrådingar

Sosiale medium er kjenneteikna ved at dei opnar for tovegskommunikasjon. Det som blir publisert, kan delast med kven som helst. Ein konsekvens av at ein fritt kan leggje ut informasjon på nettet, er mangel på førehandskontroll (kvalitetssikring). Når ein først har lagt ut informasjon, veit ein lite om kvar han blir lagra, og korleis han blir brukt i framtida. Tenestetilbydarane sikrar seg ofte høve til fri bruk av personinformasjonen som brukarane legg igjen på nettet, for eksempel til kommersielle føremål. Bruksmåtane som sosiale medium opnar for, inneber ei generell utfordring for ivaretakinga av personvernet til einskilde.

Sosiale medium opererer på ein internasjonal marknad. Brukarane er som regel lite opptekne av kva land tilbydaren tilbyr tenesta frå, men registrerer seg hos den tilbydaren som fyller det føremålet brukaren ønskjer. Dei dominerande aktørane, som Facebook og Twitter, er utanlandske. Dette set grenser for kva norske regelverktiltak ein kan setje i verk for å tryggje og styrkje personvernet for brukarane av sosiale medium.

Barn og unge er hyppige brukarar av sosiale medium, og medianalderen for debut på internett går stadig ned. Barn og unge har ikkje dei same føresetnadene som vaksne til å setje seg inn i brukarvilkår og filtrere informasjonen dei publiserer i nettmedia. Fordi dei er etablerte i utlandet, er det ei utfordring å kome i god dialog med dei sentrale tilbydarane av sosiale medium for å etablere brukarvilkår som er enklare å forstå, og som betre tek hand om personvernet til barn og unge.

Barn og unge treng særskilt vern på mange område. Dei som forvaltar barn og unge sine interesser, for eksempel gjennom å gi samtykke på deira vegner, skal handle ut frå barna sitt beste, ikkje for å eksponere seg sjølve eller fremje eigne interesser. Samstundes må det setjast av ressursar til å vidareføre og styrkje førebyggjande arbeid i form av opplysningsverksemd. Dette kan skje i regi av nasjonale koordineringsorgan, så som «Trygg Bruk»-prosjektet til Medietilsynet, eller i undervisningstilbodet på skulen. Ei rekkje norske aktørar tilbyr ulike former for hjelp i samband med publiserte opplysningar på nett eller sletting av profilar og så vidare. Fleire av desse aktørane har omfattande kontakt med barn og unge. Det kan reisast spørsmål om det bør etablerast eit eige kontaktpunkt for barn og unge, utan at det nødvendigvis reduserer mangfaldet av hjelpetilbod. Om eit slikt kontaktpunkt skal etablerast, må det gi ein vinst for brukarane ut over den ordninga ein har i dag, der brukarane sjølve må finne ut av kva aktør dei skal kontakte.

Boks 8.3 Hovudpunkt kapittel 8

- 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.

9 IKT – utsikter og utfordringar

9.1 Utviklingstrekk og trendar som verkar inn på sikringa av personvernet

Viktige teknologiske utviklingstrekk som har mykje å seie for samfunnet generelt, er auken i bruk av internett[1], sosiale medium[2], nye lagringsmedium og utsetjing av tenester, for eksempel lagring i nettskya. Desse nyvinningane representerer teknologi som er brukt av både offentleg sektor, privat sektor og folket generelt i eit omfang som det ikkje var mogleg å føreseie då dei vart lanserte. 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:

> «Den hurtige teknologiske udvikling har skabt nye udfordringer, hvad angår beskyttelse af personoplysninger. Omfanget af datadeling og -indsamling er steget drastisk. Teknologien giver både private virksomheder og offentlige myndigheder mulighed for at udnytte personoplysninger i et hidtil uset omfang, når de udøver deres aktiviteter. Fysiske personer udbreder i stigende grad deres personoplysninger offentligt og globalt. Teknologien har ændret både samfundet og det sociale liv. Opbygning af tillid i onlinemiljøet er afgørende for den økonomiske udvikling. Manglende tillid får forbrugerne til at være tilbageholdende med at købe varer på internettet og benytte nye tjenester. Dette kan forsinke udviklingen af innovative anvendelser af nye teknologier. Beskyttelse af personoplysninger spiller derfor en central rolle i den digitale dagsorden for Europa[3] og mere generelt i Europa 2020-strategien[4].»

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. I det vidare blir nokre teknologiske utviklingstrekk som kan innebere personvernimplikasjonar trekte fram. I tillegg til punkta under blir bruken av lokaliseringsteknologi drøfta nærmare i kapittel 9.4.

9.1.1 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. Den kanskje største av desse aktørane på verdsbasis er DoubleClick, som er eigd av Google. Med mange og avanserte sporingsteknologiar knytte til dei aller fleste nettsider er det nærmast umogleg å unngå å late etter seg ein stig av elektroniske spor etter aktivitetar på nettet.

Det er ikkje berre med berbare eller stasjonære datamaskiner at brukarane surfar på internett. Mobiltelefonar og smarttelefonar blir stadig viktigare plattformer når det gjeld å samle inn informasjon. Andre typar einingar, for eksempel nettbrett og e-bøker, er òg nye plattformer for innhenting av informasjon til brukarprofilering. Ei utfordring ved det at informasjonshandelen skjer på så mange ulike plattformer, er at desse har store tekniske forskjellar, og at tilgangen til gode

---

1 Statistikk frå SSB over teknologiske indikatorar frå 2005 og 2011 viser korleis tilgangen til Internett i heimen blant folket har auka. Det er snakk om ein auke frå 60 % i 2005 til 92 % i 2011.

2 I statistikken frå SSB over teknologiske indikatorar frå andre kvartal 2011 går det fram at tre av fem nordmenn bruker sosiale nettsamfunn. Aldersgruppa under 35 år er den som er sterkast representert.

3 Digital Agenda for Europa, EU sin digitale agenda: http://ec.europa.eu/information_society/digital-agenda/index_en.htm

4 Europa 2020-strategien er EUs vekststrategi for dei neste ti åra: http://ec.europa.eu/europe2020/index_en.htm#

personverninnstillingar varierer. Det er ikkje enkelt å regulere innhenting av personopplysningar på ein einskapleg måte som tek omsyn til forskjellane mellom plattformene.

Problemstillingar knytte til personprofilering og informasjonshandel som har særlege implikasjonar for personvernet, slik som framveksten av lokaliseringstenester og lagring av informasjonskapslar, er omtala i kapittel 9.4.

9.1.2 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. Ein kan i grove trekk skilje mellom tre typar nettskytenester. Den første typen er der nettskya sjølv utgjer ei programvare ferdig til bruk, som brukaren nyttar gjennom nettskytenarane. Dette kan for eksempel vere ei nettbasert e-posttenesteeller eit tekstbehandlingsprogram. Den andre er der nettskya utgjer ei plattform der brukaren kan utvikle eiga programvare, for eksempel med verktøy for og lagringskapasitet til å utvikle programvare. Den tredje typen nettskytenester er der nettskya tilbyr infrastruktur til brukaren, medan brukaren sjølv bidreg med eiga programvare. Etter denne siste modellen tilbyr nettskyleverandøren i hovudsak lagrings- og nettverkskapasitet gjennom sine eigne kraftige maskiner og store tenarparkar.

Det ligg eit stort potensial i auka bruk av nettskytenester. Den store lagringskapasiteten til tilbydarane gjer at den behandlingsansvarlege sjølv ikkje treng 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, ettersom det blir mindre behov for å lagre alt på kvar einskild maskin eller hos kvar einskild aktør. Dette kan føre til raskare og meir velfungerande lokale datasystem som er rimelegare å drifte. Nettskya er dessutan fleksibel på den måten at når den behandlingsansvarlege treng meir lagringskapasitet, leiger han det. Som regel betaler ein berre for kapasiteten som blir brukt. Dette reduserer dei store kostnadene som følgjer med store IKT-investeringar, og kan slik sett vere økonomisk gunstig særleg for mindre verksemder eller verksemder i etableringsfasen.

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. Alle dei reglane som gjeld for behandlingsansvarlege som er etablerte i Noreg og behandlar personopplysningar i Noreg, gjeld òg ved bruk av lagringstenester i nettskya. 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. Dette er fordi ein som behandlingsansvarleg ofte ikkje veit kvar dataa blir lagra. Det er heller ikkje sikkert dataa blir lagra på same staden i nettskya gjennom heile lagringsperioden, eller at alle dataa er lagra samla. 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. Datatilsynet har i 2012 behandla ei sak om Narvik kommune sin bruk av nettskytenesta Google Apps. Datatilsynet varsla opphavleg vedtak som la til grunn at Narvik kommune ikkje hadde gjort tilfredsstillande risikovurderingar, slik det krevst etter personopplysningslova § 13. Ei av utfordringane var at kommunen ikkje hadde godt nok referansegrunnlag til å kunne definere den sannsynlege faren for tryggleiksbrot, mykje på grunn av manglande informasjon frå Google. Google kunne mellom anna ikkje orientere om kvar data til kvar tid blei lagra, og kva tryggingstiltak dataa var omfatta av. Dei ville heller ikkje opplyse om kva land datasentera deira er plasserte i. Datatilsynet hevda, mellom anna på grunnlag av dei manglande opplysningane, at standardavtala som Google bruker, ikkje er tilstrekkeleg jamført med det som blir forventa av ei databehandlaravtale. Datatilsynet oppfordra kommunen til å greie ut saka nærmare og få meir detaljerte opplysningar frå Google før dei inngår ei databehandlaravtale med

selskapet. Kommunen har på nytt vore i dialog med Google. Dei kan no mellom anna vise til ei avtale med Google om jamlege revisjonar av tryggingssystema knytte til tenesta, som ein uavhengig tredjepart utfører. Kommunen gjer deretter risikovurderingar ut frå desse revisjonane. Etter å ha gjennomgått den siste utgreiinga frå kommunen godkjende Datatilsynet i september 2012 avtala med Google om å bruke Google Apps.

Det kan tenkjast at mange behandlingsansvarlege, særleg små og mellomstore verksemder, vil få betre trygging av personopplysningar når dei bruker nettskytenester. Dei store leverandørane av nettskytenester har langt betre sikra tenarparkar, høgare IT-kompetanse og betre rutinar for sikring av personopplysningar enn dei behandlingsansvarlege sjølve er i stand til å oppnå. Utfordringa er å finne løysingar på dei informasjonsbarrierane som hindrar tenesteleverandørane i å dokumentere tryggleiksnivået overfor kunden. Ei løysing med jamleg revisjon av ein uavhengig tredjepart, slik Google og Narvik kommune har avtala, kan vere ei mogleg løysing på dette problemet. Det føreset at revisjonen tek føre seg alle dei nødvendige aspekta.

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. 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[5]. For det første ønskjer dei å finne fram til ein felles standard for nettsky. For det andre ser dei det som nødvendig å utvikle sikre og balanserte kontraktsvilkår for nettsky. Endeleg har dei sett seg som mål å etablere eit felles europeisk partnarskap i offentleg sektor som skal sikre innovasjon og vekst i utviklinga av nettskyteknologi.

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.

9.1.3 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. Særleg i samband med tilgangskontroll er det fordelar knytte til bruken av teknologi for måling av biologiske mønster. Bruken av biometri gjer at ein mykje sikrare kan identifisere eller autentisere ein person enn for eksempel ved bruk av passordløysingar, som ikkje er uløyseleg knytte 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. Alle har sine biometriske eigenskapar, og dei er òg som regel lette å vise fram. Enkelte biometrimetodar er det lettare for folk å godta enn andre. For eksempel kan det hende at folk synest at det å få andletet avlese ikkje er eit like stort inngrep i integriteten som det å få avlese fingeravtrykk[6]. På den andre sida kan enkelte biometrimetodar opplevast som eit særleg stort inngrep i inte-

---

[5] European Commission: Unleashing the Potential of Cloud Computing in Europe. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussel, 27.09.2012.

[6] Yue Liu, Nancy: Bio-Privacy. Privacy Regulations and the Challenge of Biometrics. Routledge, 2012. s.30 flg.

griteten, 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. Biometriske eigenskapar (hovudsakleg fingeravtrykk) blir registrerte på ein enkelt identitet og knytte til passet til vedkomande. På denne måten sikrar ein at ikkje fleire individ reiser på same pass, og at ikkje ein person kan bruke ulike pass ved ulike reiser. Bruken av biometri i pass gjer òg at det er vanskelegare å forfalske pass utan at det blir oppdaga. Biometri blir brukt i automatiske grensekontrollar (e-gates) og er både sikrare og meir effektivt enn dagens manuelle grensekontroll. 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 [7].

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. Kameraa er knytte til program som analyserer andlet og mellomlagrar malar av dei. Dei mellomlagra andleta blir deretter samanlikna mot ein database av allereie registrerte (og identifiserte) andlet for å finne ut om nokon av dei nye andleta tilhøyrer personar som av ulike grunnar er registrerte i systemet til databehandlaren. Eit mogleg bruksområde for denne teknologien er flyplassar. Her kan metoden for eksempel brukast til å registrere om kriminelle personar eller personar utan autorisert tilgang oppheld seg på dei overvaka områda. «Face in the crowd»-teknologi har mellom anna vore testa ut ved flyplassen Keflavik på Island og under amerikanske Superbowl tidleg på 2000-talet.

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. Desse måla for attkjenning (silhuett og rørsler) kan lagrast i eit register som ein mal for ein bestemt, ikkje-identifisert person. Ein mann vart i 2008 dømd til to års fengsel i Bolton Crown Court i Storbritannia for eit innbrot han hadde gjort seg skuldig i. Ganglagsbiometri vart brukt som bevis i saka. Ein fotspesialist kjende att ganglaget til mannen frå ulike overvakingskamera, og DNA-et samsvara med det som vart funne på åstaden. Ganglagsbiometri kan brukast i etterforskinga av kriminelle handlingar ved at ein analyserer og samanliknar ulike videoopptak frå overvakingskamera for å finne fram til personar som har vore på eller nær åstaden.

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. Det er òg ein viss fare for at biometriske malar som blir lagra i eit register, kan førast tilbake til dei opphavlege biometriske dataa. Dette kan gjerast ved å rekonstruere det biometriske trekket (for eksempel eit fingeravtrykk) som vart brukt til å lage malen. Dette går under namnet «biometri-spoofing». Når ein bruker biometriske eigenskapar til identifisering og autentisering, blir desse eigenskapane omsette til tal i ein database gjennom fleire ledd. Her er det viktig at biometrien blir godt sikra med PKI-baserte sertifikat[8].

Ytre faktorar kan medverke til å redusere kvaliteten på dei biometriske dataa eller samanhengen mellom data og person. Dei fysiske omgivnadene (varme, fukt og liknande) kan ha mykje å seie for kor gode data ein får på registreringstidspunktet. Det er derfor ein viss feilmargin knytt til bruk av biometri. Det kan oppstå situasjonar der ein biometrisk eigenskap, for eksempel eit fingeravtrykk, feilaktig blir knytt til identiteten til ein annan person av di den opphavlege registreringa var av låg kvalitet. Feil kan òg skje dersom den automatiske samanlikninga av eigenskapen som blir presentert, og den som er registrert, ikkje er god nok.

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. Bruk av teknologien baserer seg ikkje på samtykke, og dette kan vere problematisk i den perioden alle dei skanna andleta er lagra for å bli samanlikna med registrerte andlet. Det kan òg tenkjast at visse typar biometriske data kan avsløre sensitiv informasjon, til dømes om helsetil-

[7] PVN 2011-11 Visma Retail.

[8] PKI (Public Key Infrastructure) er nærmare omtalt i kapittel 9.5.1.

stand. Eit fingeravtrykk kan for eksempel brukast av rettsmedisinarar til å lage ein DNA-profil. Det er derimot ikkje ofte det lèt seg gjere å utleie medisinske diagnosar på denne måten.

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». På bakgrunn av dette har dei mellom anna godteke bruken av fingeravtrykksmalar som er knytte til treningskort til bruk på døgnopne, ubemanna treningssenter[9]. Dei har òg godteke ei løysing for autentisering av myndige personar ved hjelp av fingeravtrykksmalar som er knytte til fødselsdato, til bruk i ein ubemanna daglegvarebutikk[10]. 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.

[9] PVN-2011-12 Adgangskontroll ubetjent treningssenter.

[10] PVN-2011-11 Visma Retail.

9.2 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.

9.2.1 Teknologinøytral lovgiving

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. Teknologinøytralitet tilseier derfor at lovgivinga til kvar tid skal vere nøytral med omsyn til teknologi og utvikling. Dersom ein har ei teknologinøytral lovgiving, sikrar ein at det i regelverket ikkje blir diskriminert mot enkelte typar teknologiar, eller at ikkje enkelte teknologiar får fordelar framfor andre.

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. God infrastruktur inneber at ein innstiller seg på teknologisk utvikling. Dersom ein i størst mogleg grad bruker teknologinøytrale omgrep i lovgivinga, unngår ein at det oppstår situasjonar der teknologiar som i prinsippet har dei same funksjonane og personvernkonsekvensane, er ulike for lova.

9.2.2 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. Innebygd personvern tyder ikkje berre at personvern er ein del av arkitekturen til kvar enkelt teknologi. Det tyder òg – på eit overordna plan – at personvern er ein naturleg del av alle systema innbyggjarane møter i kvardagen.

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. Men i ein digital tidsalder er ikkje lovgiving og regulering tilstrekkeleg for å kunne sikre personvernet. Privatpersonar og kommersielle aktørar må arbeide for å integrere personvern i det daglege arbeidet. Ein bør derfor ha eit prinsipielt mål om innebygd personvern i alle sektorar, og offentlege styremakter bør vere blant dei fremste pådrivarane for å realisere dette prinsippet.

Situasjonar der innebygd personvern med fordel kan takast i bruk, er når ein skal utvikle nye register. Personvern bør spele ei viktig rolle allereie på planleggings- og lovgivingsstadiet. Deretter bør det følgjast opp på utviklingsstadiet og i bruken av registera.

Særleg om ordninga med e-resept

Eit godt eksempel på innebygd personvern er innføringa av ei ordning med elektroniske reseptar (e-resept) i Noreg. Ordninga inneber at pasientar ikkje lenger får resepten utskriven på papir. Legen sender resepten elektronisk til ein sentral database, Reseptformidlaren. Herifrå kan apoteket eller bandasjisten opne resepten og ekspedere han når pasienten kjem for å få utlevert det legen har skrive ut.

Elektroniske reseptar er regulerte av ei eiga forskrift med heimel i helseregisterlova, reseptformidlarforskrifta. Reseptformidlaren er eit ikkje-historisk helseregister der reseptar blir lagra mellombels fram til dei er ferdig ekspederte, trekte tilbake av legen eller utgått på dato. Forskrifta regulerer i detalj kva Reseptformidlaren kan innehalde av opplysningar. E-reseptar er elektronisk signerte av legen, og det blir kontrollert om dei er ekte. Ein kan derfor vere svært trygg på at det ikkje dukkar opp falske reseptar. Vidare står det i forskrifta kven som skal kunne få tilgang til opplysningane, og på kva vilkår. Reseptformidlaren er ikkje eit samtykkebasert helseregister etter helseregisterlova, men tilgang til opplysningane i registeret er basert på samtykke frå pasienten. Ein resept i Reseptformidlaren er berre tilgjengeleg for den som behandlar resepten. All aktivitet i Reseptformidlaren blir logga. Systemet registrerer kven som opnar resepten, og kva som blir gjort med han. Dersom det blir gjort oppslag i Reseptformidlaren som ikkje fører til at det blir utlevert legemiddel, blir dette logga på ein særskild måte, ettersom det kan tyde på ureglementert tilgang.

Dersom ein pasient ønskjer å verne opplysningane sine ekstra godt, kan vedkomande velje ein låst resept. Ein låst resept kan berre søkjast opp med referansenummeret til resepten. Pasienten kan be om å få låst resept hos legen og får då skrive ut referansenummeret. Nummeret må visast fram på apoteket eller hos bandasjisten for å få ekspedert resepten. Ein låst resept er teknisk sperra for opning frå andre enn den som kjenner referansenummeret.

For å styrkje personvernet ytterlegare har forskrifta reglar om at opplysningar ikkje kan leverast ut til arbeidsgivar, til påtalemakt/domstol eller til forskingsføremål, sjølv om den registrerte samtykkjer i det. Fleire av helseregistera som er heimla i helseregisterlova, har eit slikt forbod mot gjenbruk.

Personvern er ein del av arkitekturen i løysinga, mellom anna på den måten at e-resept-funksjonaliteten er integrert i fagsystema til legar og apotek. Reseptformidlaren, reseptutskrivarane, apoteka og bandasjistane er òg knytte til Norsk helsenett. Dei er forplikta til å følgje Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren (Norma).

Innebygd personvern som mål

Prinsippet om innebygd personvern er samansett. Når ein utviklar IKT-system og annan informasjonsteknologi, bør ein for det første sørgje for å velje tekniske løysingar som gir best mogleg informasjonstryggleik og vern av personopplysningar. 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. På denne måten er brukaren sikra eit best mogleg personvern sjølv om han eller ho ikkje gjer nokon endringar i førehandsdefinerte brukarinnstillingar.

Bruk av teknologi bør skje på ein måte som fremjar personvernet. Ved å stille krav til informasjon om teknologien som blir brukt, til behandlinga av personopplysningar og til kven som har

tilgang til opplysningane, og dessutan ved å gi klåre reglar om føremålet kan ein sørgje for at brukaren nyttar teknologien på ein medviten måte for å sikre sitt eige personvern. Kunnskap og medvit er ein spesielt viktig del av prosessen med å byggje personvernet inn i alle dei systema innbyggjarane møter i kvardagen. Ein føresetnad for at teknologien blir brukt bevisst, er at brukaren faktisk forstår problematikken rundt personvern. Større kunnskap blant folk om personvern og konsekvensane av dårleg personvern er med andre ord ein føresetnad for innebygd personvern. Ein del av prosessen med å oppnå innebygd personvern handlar derfor 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. Brukarvenlege opplegg må vere eit mål for alle aktørar, og 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. 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.

9.2.3 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. Dataminimalitet er slik sett hovudføremålet med desse teknologiane. 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. Dersom ein får på plass innebygd personvern i alle teknologiar og praksisar, har ein ikkje behov for eigne PETs. Mykje talar derimot for at ein i framtida kjem til å trenge begge løysingane.

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). Denne funksjonen «immuniserer» personopplysningar, slik at søkjemotoren ikkje får treff på namnesøk i dokument som har vore lagra i meir enn tolv månader. Slik søkjemotorimmunisering vart tilrådd av Personvernkommisjonen i 2009, og det kan vere aktuelt å implementere det i andre søkjemotorar òg.

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. Dei ønskjer òg å utarbeide standardmekanismar som dei ulike nettaktørane kan bruke for å fortelje brukarane at dei faktisk respekterer ønsket deira om ikkje å bli spora. Gruppa har som mål å lage ei tilråding til ein «do not track»-standard innan utgangen av april 2013. Svært mange av dei store internasjonale aktørane, mellom andre Microsoft, Apple og IBM, deltek i arbeidet, i tillegg til forskarar og representantar frå ulike interessegrupper for personvern. Arbeidet til gruppa har fått positiv respons frå EU-hald. EU-kommisjonen ønskjer meir fokus på «do not track»-teknologi, og stør initiativa til å utarbeide ein standard for «do not track»[11]. 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.

[11] Neelie Kroes: Online privacy: reinforcing trust and confidence. Tale attgitt i pressemelding 22. juni 2011.

9.2.4 Bruk av standardar/bransjenormer

Det er spesielt viktig å utarbeide standardar og bransjenormer som tek omsyn til personvernet. 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. Det er allereie fleire gode eksempel på bransjenormer og standardar som er utarbeidde med tanke på å betre personvernet i bestemte sektorar.

Bransjenorm for personvern og informasjonstryggleik i elektronisk billettering

Eit mål i kollektivtrafikken er å sørgje for at kundane kan bruke eitt og same reisekort uavhengig av reisestrekning og transportselskap. Reiser med elektroniske billettar som er identifiserande, og spesielt billettar som kan brukast på tvers av transportselskapa, gir ei rekkje utfordringar med omsyn til personvern. Kollektivtransportbransjen tok derfor sjølv initiativ til å utvikle ei bransjenorm for elektronisk billettering, som forpliktar aktørane til å sikre personvernet til alle som bruker elektroniske billettar. Bransjenorma for elektronisk billettering i kollektivtransporten vart innført ved årsskiftet 2011/2012. Ho skal medverke til at alle kundar som bruker elektronisk billett, kan reise anonymt med båt, buss, bane og tog dersom dei føretrekkjer det. Trafikantar som reiser anonymt skal få tilgang til dei same fordelane og den same servicen som trafikantar som vel å inngå personlege avtaler med transportselskapet. Det er viktig at det ikkje skal hefte ulemper ved det å velje anonyme løysingar framfor løysingar som inneber at passasjeren kan sporast. Bransjenorma legg til rette for at utviklinga av betalingsløysingar skal skje på ein personvernvenleg måte.

Norm for informasjonstryggleik i helse- og omsorgssektoren

Bransjenorma for informasjonstryggleik i helse- og omsorgssektoren vart utarbeidd i juni 2010 av representantar for helsesektoren og er bindande for alle private og offentlege verksemder som er knytte til Norsk helsenett.

Føremålet med norma er å få tilfredsstillande informasjonstryggleik i sektoren. Ho er òg meint å skulle vere eit hjelpemiddel til kvar enkelt verksemd i arbeidet med informasjonstryggleik. I norma blir det stilt krav som detaljerer og supplerer det gjeldande regelverket. Dersom desse krava blir oppfylte, oppfattar sektoren det slik at krava om tilfredsstillande informasjonstryggleik i det gjeldande regelverket òg er oppfylte. Norma og krava som norma omfattar, blir juridisk bindande ved avtale, i den grad innhaldet ikkje allereie går fram av lov eller forskrift.

Norma er først og fremst basert på kravet i personvern- og helselovgivinga om at ein må etablere tilfredsstillande informasjonstryggleik for system som inneheld helse- og personopplysningar, jf. personopplysningslova § 13, helseregisterlova § 16 og personopplysningsforskrifta kapittel 2. Norma dekkjer alle verksemdene i helse- og omsorgssektoren i tillegg til arbeids- og velferdsetaten. Men ho kan òg ha stor overføringsverdi som mal for andre sektorar. Totalt gjeld norma for frå 20 000 til 27 000 verksemder, alt frå store Oslo universitetssjukehus HF og Nav-kontor til små legekontor, tannlegeklinikkar, fysioterapiklinikkar og apotek.

Norma inneber ei konkretisering av dei generelle personvernreglane som gjeld for helse- og omsorgssektoren etter personopplysningslova, personopplysningsforskrifta og helseregisterlova. Mellom anna inneber norma at det blir stilt konkrete krav til kva ei risikovurdering etter personopplysningsforskrifta § 2-4 skal innehalde, og kva reglar som skal gjelde for autorisering, tilgangsstyring og autentisering. Det er allereie gjennomført omfattande opplæringstiltak i samband med norma, og det blir no førebudd kurs og instruktørutdanning for stadig fleire delsektorar.

9.3 Informasjonstryggleik og personvern

Informasjonstryggleik er eit viktig verkemiddel for å sikre godt personvern. God informasjonstryggleik er òg ein føresetnad for at digitale tenester blir tekne i bruk. Tilfredsstillande rammer rundt det å samle inn og behandle personopplysningar gir nødvendig tillit og gjer behandlinga påreknelig for alle partar.

Eit overordna bilete av dagens situasjon når det gjeld informasjonstryggleik i Noreg, er gitt i stortingsmeldinga om samfunnstryggleik[12]. I kapittel 9 om IKT-tryggleik skisserer regjeringa ei rekkje utfordringar og trendar som kan påverke informasjonstryggleiken. For å møte desse utfor-

[12] Meld. St. 29 (2011-2012) Samfunnssikkerhet.

dringane blir fleire overordna tiltak for å styrkje informasjonstryggleiken i samfunnet lanserte.

For å møte tryggleiksutfordringane på IKT-området har regjeringa laga ein nasjonal strategi for informasjonstryggleik. Strategien peiker på kva retningsval og kva prioriteringar som skal liggje til grunn for arbeidet styremaktene skal gjere for å få betre informasjonstryggleik i åra som kjem. I samband med gjennomføringa av strategien kan fylkeskommunar, kommunar og verksemder i privat sektor involverast i konkrete tiltak.

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: Kva trugsmål er verksemda utsett for, kor sårbar er verksemda overfor desse trugsmåla, og kva konsekvensar vil eit eventuelt tryggleiksbrot få? Risikovurderinga fører ofte til at ein oppdagar eit behov for å heve tryggleiksnivået.

9.3.1 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. Ein kan for eksempel verne om konfidensialiteten ved å styre tilgangen til personopplysningane på ein effektiv måte, gjennomføre fysiske tryggingstiltak, opprette brannmurar og liknande. Tilsvarande kan ein sikre tilgangen ved å bruke avbrotsfri straumforsyning, alternativ tilgang til nettverk og liknande.

Mangel på god informasjonstryggleik i ei verksemd kan føre til at tilliten hos den registrerte og samarbeidande verksemder blir redusert. For private verksemder kan dette innebere at kundeforholdet eller samarbeidet blir avslutta, medan det for offentlege verksemder kan føre til at innbyggjaren blir mindre villig til å dele personopplysningar med verksemda. For begge typane verksemder kan uansvarleg handtering av personopplysningar føre til erstatningsansvar og tap av omdøme.

9.3.2 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. Her finn ein mellom anna reglar for kva plikter verksemder har til å setje i verk sikringstiltak.

Ei anna form for kontrolltiltak er dei av økonomisk art. Om ein innfører økonomiske fordelar for aktørar som gjennomfører sikringstiltak, vil verksemder ha ei økonomisk interesse av å vere opptekne av informasjonstryggleik. 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. Dette blir drøfta nærmare i kapittel 9.5.

Informasjonstiltak og haldningsskapande arbeid

Informasjonstiltak er òg eit viktig verkemiddel for å oppnå god informasjonstryggleik. Mange verksemder manglar som nemnt kompetanse på området, særleg mindre verksemder som ikkje har IKT som hovudarbeidsområde, men som likevel behandlar informasjon elektronisk og dermed har plikt til å sikre informasjonen mot misbruk. Det er viktig at denne typen verksemder har tilgang til god informasjon og eit hjelpeapparat når dei har spørsmål om informasjonstryggleik. Det er for eksempel ikkje enkelt å setje seg inn i alle moment som bør vere med i ei risikovurdering. Derfor bør verksemder som treng informasjon om og hjelp til å gjennomføre slike vurderingar,

ha tilgang til det. 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. Dette er eit haldningsspørsmål. Ei fornuftig haldning til informasjonstryggleik krev at ein har god kunnskap både om tilgjengelege tiltak og motiva for dei ulike tiltaka. 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 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. Dess meir informasjon som er samla, og dess fleire delar i eit informasjonssystem som er avhengige av kvarandre, dess enklare er det å finne ein veg inn i (og ut av) systemet. 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)*. Sjølv om det er vanskeleg i større informasjonssystem å til kvar tid ha få pålitelege komponentar, er dette likevel noko ein bør ha som mål.

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. Denne typen programvare kan for eksempel vere *brannmurar, tryggingsfilter og applikasjonar* eller *antivirusprogram*. Alle informasjonssystem bør ha slike sikringstiltak.

Løysingar for *avbrotsfri straumforsyning* kan bidra til å sikre tilgangen til eit system. Slike løysingar kan for eksempel vere batteri eller andre elektriske apparat som forsyner system med straum når straumbrot oppstår. Ei anna løysing som kan sikre tilgangen til eit system, er bruk av *alternative nettverk*, slik at ein kan logge seg på også i situasjonar der hovudnettverket er nede eller har vore utsett for hacking. Det er viktig at ein nyttar denne typen tiltak i større informasjonssystem.

Kryptering av viktig informasjon og kommunikasjon er ein tryggleiksføresetnad for større, meir kompliserte og dermed òg meir sårbare informasjonssystem. Ved å kryptere kommunikasjonen kan ein sende informasjon over infrastrukturar sjølv om dei er usikra, fordi informasjonen blir gjord utilgjengeleg for uvedkomande. Dei to alternative metodane for kryptering er kanalkryptering og innhaldskryptering. Kanalkryptering går ut på å kryptere kommunikasjonslina mellom avsendar og mottakar, slik at uvedkomande for eksempel ikkje kan avlytte kommunikasjon over nettverket. Innhaldskryptering består i å kryptere innhaldet i kommunikasjonen, for eksempel ved å kryptere innhaldet i ein e-post, slik at berre ein mottakar som har nøkkelen til å dekryptere informasjonen, får lese han. Innhaldskryptering er ikkje avhengig av at kommunikasjonen skjer over sikra nettverk. Dette inneber for eksempel at ein kan sende ein sensitiv arbeidsrelatert e-post frå ein internett-kafé utan å risikere tryggleiksbrot. Det gir betre personvern og tryggleik å bruke innhaldskryptering framfor kanalkryptering. Dette er derimot meir kostbart og tidkrevjande, ettersom det trengst ein ekstra operasjon både hos avsendaren og hos mottakaren når ein e-post skal krypterast og dekrypterast.

System for *identitetsforvalting, tilgangskontroll og logging* er blant dei viktigaste teknologiske verkemidla for informasjonstryggleik. Identitetsforvalting inneber å handtere opplysningar om kven nokon er, og kva rolle denne personen har. Tilgangskontroll er ein måte å sikre informasjonssystem på, for eksempel gjennom passordløysingar og liknande løysingar for autentisering og differensiering av tilgangsnivå og brukarroller. Tilgangskontroll sikrar også at rett person har tilgang til relevant informasjon til rett tid. Logging er eit tryggingstiltak som inneber å etterkontrollere informasjonssystem. Det er viktig å skilje mellom nettverksbasert logging og innsynslogging. Den nettverksbaserte logginga inneber at dataflyten inn i og ut av nettverket blir logga. Dette kan medverke til at datainnbrot og virus blir oppdaga, og at mistenkjelege typar datatrafikk kan oppdagast og undersøkjast nærmare.

Innsynslogginga (som på fagspråket blir kalla klientbasert logging) er den som skjer internt i eit system. Innsynslogging omfattar mange ulike

typar loggar. Typiske innsynsloggar er dei «som dokumenterer vellykkede og mislykkede innloggingsforsøk, brudd på rettigheter tildelt brukeren, oppnådd adgang til filområder, og andre hendelser på systemet»[13]. Med klientbasert logging kan ein mellom anna avdekkje såkalla «snoking» i registera.

Problemstillingar som gjeld identitetsforvalting, tilgangskontroll og logging blir nærmare omtala i kapittel 9.5.

9.3.3 Utfordringar

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. Verksemdene må føle at tilsynsstyremakta er til stades ved at det blir gjennomført kontrollar. Dette er viktig for å sikre at det ikkje skal løne seg å neglisjere regelverket. Styremaktene må vere tilgjengelege for å gi rettleiing til verksemder som treng spesiell støtte for å etterleve regelverket. Vidare må styremaktene gi god allmenn informasjon som kan stø opp under prosessane i verksemdene, og verksemdene må få hjelp med å leggje til rette gode teknologiske løysingar for informasjonstryggleik.

Det er òg viktig at ein med jamne mellomrom drøftar behovet for nye sikringsmetodar for IKT-systema i både offentlege og private verksemder. Andre moglege tiltak for å sikre informasjonstryggleiken og personvernet knyter seg til system for identitetsforvalting og logging. Desse blir presenterte i kapittel 9.5.

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.

9.4 Elektroniske spor

Nordmenn lever i aukande grad i ein teknologisk og interaktiv kvardag. Ein bruker e-post både privat og på jobb, deltek i sosiale nettverk, kjøper varer på nett og med bankkort, bruker GPS i bilen og på mobilen og googlar informasjon om alt frå medisinske diagnosar til neste feriemålet. Heile dagen igjennom lèt innbyggjarane etter seg ein stig av elektroniske spor.

Desse spora kan følgjast av ulike aktørar. Politiet får mellom anna rett til å hente inn telefonloggar og IP-loggar under gitte føresetnader. Finansinstitusjonar har oversikt over kor mykje pengar ein bruker, og når, kvar og korleis ein bruker dei. Sosiale nettverk kan vise annonsar som er spesialtilpassa profilen til den enkelte etter analysar dei har gjort av åtferda i nettverket.

Samfunnet blir meir og meir avhengig av å ha velfungerande elektroniske kommunikasjonsnett og -tenester. Innbyggjarane utfører stadig fleire tenester ved hjelp av elektronisk kommunikasjon, og trafikkmengda i elektroniske kommunikasjonsnett aukar. 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», det vil seie at vi lever i eit samfunn der det uunngåeleg eksisterer enorme sett med data knytte til kvar enkelt person og rørslene, vala og kommunikasjonen hans eller hennar. Eit viktig spørsmål alle bør stille seg, er kva opplysningar som blir innsamla, av kven og til kva føremål. Nedanfor blir det gjort greie for nokre av dei mest aktuelle teknologiane for datainnsamling ved hjelp av elektroniske spor.

9.4.1 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. I visse delar av sektoren har dei òg teke aktivt i bruk detaljregistreringar i form av ferdsskrivarar, gravitasjonssensorar som registrerer akselerasjon, nedbremsing og gravitasjonskrefter i svingar, og dessutan køyrecomputarar, for eksempel for å sjå korleis sjåførane utfører arbeidsoppgåvene sine. Ein annan og meir omfattande type geolokalisering skjer ved hjelp av GPS eller gjennom å analysere IP-adres-

[13] NorCERT kvartalsrapport for 4. kvartal 2011 på s. 15.

ser. Ekomtilbydarar verda over gjer dette dagleg, ettersom det i dag er mogleg på grunn av den omfattande bruken av smarttelefonar.

Det er i hovudsaka tre typar aktørar som registrerer lokaliseringsdata: ekomtilbydarar, internettleverandørar og enkelte andre internett-aktørar. Ekomtilbydarane har tilgang til lokaliseringsdata gjennom basestasjonane dei kontrollerer. Ofte er ekomtilbydarane internettleverandørar i tillegg, slik som Telenor og NetCom, og desse har òg tilgang til lokaliseringsdata gjennom dei trådlause nettverka og IP-adressene dei administrerer. Det er òg mogleg for andre internett-aktørar, for eksempel program- og applikasjonsleverandørar, å finne fram til kvar brukarane oppheld seg. Dette kan dei gjere ved å analysere IP-adressa til brukaren eller ved å analysere andre unike identifikatorar knytte til det utstyret brukaren er kopla til nettet med.

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. Dette inneber at lokaliseringsinformasjon for ei mobil eining ofte er å rekne som personopplysningar. 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. Artikkel 29-arbeidsgruppa har kome med ei fråsegn om geolokalisering av smarttelefonar[14]. Gruppa peiker mellom anna på at teknologien gir større risiko for at ein arbeidsgivar overvakar dei tilsette. Dei understrekar òg at dei teknisk moglege måtane å overvake telefonen på utan å informere eigaren er urovekkjande.

Eit anna viktig tema er geolokalisering av barn. Teknologien gjer det mogleg for foreldre å GPS-spore sine eigne barn gjennom smarttelefonane deira. Tele2 har lansert eit mobilabonnement for barn som kan administrerast av foreldra eller andre ressurspersonar. Abonnementet inneber mellom anna at foreldra kan avgjere kven barnet kan ringje til og når, og dessutan kor mange ringjeminutt eller meldingar barnet har lov til å bruke på dei ulike kontaktgruppene, for eksempel vener og familie. Det er òg mogleg for foreldre å lokalisere mobiltelefonen til barna. 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.

Ut ifrå personvernomsyn er det klårt å føretrekkje at lokaliseringstenester blir aktiverte av brukaren sjølv, og at aktive lokaliseringstenester ikkje er del av dei førehandsdefinerte innstillingane på telefonar, nettbrett og anna utstyr. I tillegg kan ein kanskje styrkje personvernet ved å innføre jamlege påminningar om at brukaren har aktivert lokaliseringstenester, saman med ei rettleiing om korleis vedkomande kan slå av desse tenestene.

9.4.2 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. Både i offentlege transportsystem, som buss og t-bane, og i bompengeanlegg er det lagra opplysningar knytte til dei reisande i form av tilgangskontrollar, tidsstempling og passeringsdata. Når det gjeld kollektivtransporten, hadde ein ved innføringa av elektroniske reisekort i mange norske byar ein debatt rundt graden av anonymitet som desse elektroniske korta kunne tilby dei reisande. Etter at det kom fram at det vart lagra svært detaljert informasjon om reiseruter og reisetider som kunne knytast direkte til dei reisande, oppstod det ein debatt om moglege anonyme løysingar også for dei elektroniske reisekorta. Dette førte til at ei bransjenorm for personvern og informasjonstryggleik innan elektronisk billettering vart innført ved årsskiftet 2011/2012, slik det er nemnt i kapittel

[14] Opinion 13/2011 on Geolocalisation services on smart mobile devices (WP 185).

9.2.4. 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. Dette gjer det vanskeleg å ferdast anonymt, ettersom alle bilar som passerer, lèt etter seg informasjon om kven som har betalt for passeringa, tidspunktet for passeringa og nøyaktig kvar passeringa skjedde. Det er dei same dataa som blir lagra uansett kva type køyretøy som passerer. Dette inneber at anten ein passerer som privatperson eller i tenestesamanheng, blir dei same opplysningane lagra. I samsvar med vedtak i Personvernnemnda[15] blir passeringsdata lagra i ti år. Det finst per i dag eit såkalla «sporfritt alternativ», der passeringsdata maksimalt blir lagra i 72 timar. Ein kan velje dette alternativet når ein inngår ei AutoPASS-avtale. Passeringane blir då krypterte etter maksimalt 72 timar. Lokalisering og datoar blir fjerna, slik at det einaste som blir liggjande att i systemet, er namnet på bileigaren og talet på passeringar. 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*.

9.4.3 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. Desse brikkene blir for eksempel bygde inn i produkt som elektronikk og fraktpallar i varehus av ulike typar til sporingsføremål. Det finst forskjellige typar RFID-brikker som kan sporast i varierande grad og ved hjelp av ulike metodar. Såkalla *aktive* RFID-brikker sender sjølve ut elektromagnetiske bølgjer. Desse kan avlesast på ein bestemt radiofrekvens frå RFID-basar som ligg i nærleiken av den staden der brikka til kvar tid er. Dei *passive* RFID-brikkene er derimot dei mest brukte, og dei sender berre ut signal dersom dei blir aktiverte med signal frå ein sendar. Slike sendarar sender signal over svært korte avstandar. For å kunne registrere dei fleste av desse brikkene må dei vere svært nær ein avlesar.

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. I Frankrike har ein teke i bruk NFC-teknologien for å utvikle eit nytt betalingssystem for trikkesystemet i Nice, og i Strasbourg planlegg ein å ta i bruk det same. Dei reisande får kjøpt eigne smarttelefonar som er knytte til trikkeselskapet, og registrerer reiser ved å halde telefonane tett opp mot registreringseiningane. Reiserekninga får dei saman med telefonrekninga. Dei har òg visse rabattsystem for butikkar knytte til telefonane, noko stadig fleire lokale butikkar deltek i. Det er planlagt å implementere teknologien for transportsystemet i London i løpet av 2013, og visse norske aktørar har òg testa ut NFC-teknologi med tanke på betaling gjennom smarttelefonar. 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 brikkene, 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

[15] PVN 2010-7 Passeringsdata E18 Vestfold, PVN 2010-8 Passeringsdata Fjellinjen.

avlesaren. Dette gjer at kommunikasjonen blir sårbar for angrep, for eksempel avlytting, modifisering av data og svindel. Dersom det er personopplysningar (for eksempel kontoopplysningar og kontaktinformasjon) knytte til kommunikasjonen, vil dette utgjere eit potensielt trugsmål for personvernet til brukarane.

9.4.4 Lagring av informasjonskapslar

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. Frå innhaldet i informasjonskapslar kan ein utleie opplysningar om alt frå besøkstidspunktet og lengda på besøket til lokalisering, referansesider (kvar brukaren kom seg til nettsida frå i utgangspunktet), søkjeord og kva delar av nettsida brukaren besøkte. Ein skil gjerne mellom informasjonskapslar som blir lagra mellombels, og dei som blir lagra varig, og vidare mellom informasjonskapslar lagra av ein førstepart (nettsida brukaren besøkjer) eller ein tredjepart (ofte samarbeidspartnarar eller annonsørar med koplingar til førsteparten). Det er dei varige informasjonskapslane som blir lagra av tredjepartar som byr på størst problem for personvernet.

Eit spørsmål som ofte kjem opp når ein drøftar informasjonskapslar i eit personvernperspektiv, er om kapslane inneheld personopplysningar. Personopplysningar er opplysningar og vurderingar som kan knytast til ein enkeltperson, dette følgjer av personopplysningslova § 2 nr. 1. Alle informasjonskapslar og opplysningane som blir lagra i kapslane, kan knytast mot unike identifikatorar i kommunikasjonsutstyret dei blir lagra i. 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. 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. Informasjonskapslane blir i tillegg brukte til å gjenopprette vindauge som er lukka ved ein feil, og til å setje språkinnstillingar for ei nettside, slik at brukarane straks kan lese nettsida på sitt eige språk. Mykje av logginga på nettsider skjer òg ved hjelp av informasjonskapslar. Det er viktig å merke seg at det ikkje er absolutt teknisk nødvendig å lagre informasjonskapslar for at nettsider skal fungere. Kapslane medverkar likevel ofte til å gjere sidene meir brukarvenlege, for eksempel ved at ein kan aktivere tenester for automatisk innlogging. Likevel er det er 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. Brukarane har til ein viss grad høve til å slette denne typen informasjonskapslar frå nettlesaren. Den tidlegare nemnde «do not track»-standarden kan òg bidra til at brukarane får betre kontroll over lagringa av informasjonskapslar på sitt eige utstyr dersom standarden blir implementert. 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». 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. Det er òg lite truleg at dei som lagrar denne typen informasjonskapslar, i nokon særleg grad vil respektere eit ønske frå brukarane etter «do not track»-standarden.

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. Der kravet tidlegare har vore at brukaren berre skal informerast om lagringa av desse typane informasjonskapslar, er det bestemt at den behandlingsansvarlege i tillegg skal hente inn samtykke frå brukaren ved slik lagring. Dette kan mellom anna ramme aktørar som driv med interaktiv reklame.

Artikkel 29-arbeidsgruppa har i ei fråsegn om samtykke til lagring av informasjonskapslar[16] uttala seg om kva typar lagringsføremål dei meiner vil krevje samtykke frå brukarane etter artikkel 5 (3), og kva føremål som fell inn under unntaket for lagring som er teknisk nødvendig. Blant føremåla som etter 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.

9.5 Identitetsforvalting: identifisering, autentisering og tilgangsstyring

Det finst inga plikt til å ha med seg legitimasjonsbevis til dagleg i Noreg. Likevel er det vanleg at ein i ulike situasjonar må godtgjere alder, namn og liknande. Derfor har dei fleste eit fysisk legitimasjonsbevis med seg. Både overfor offentlege styremakter og private verksemder må enkeltpersonar i mange tilfelle godtgjere identiteten sin ved å vise fram for eksempel pass, bankkort eller førarkort for å få tilgang til rettar eller tenester. Ved bruk av elektroniske tenester er det òg behov for identitetskontroll. Enkeltpersonar kan då nytte elektroniske identitetsbevis (e-ID), slik som MinID, BankID eller Buypass e-ID.

I IKT-system der store mengder personopplysningar blir behandla, er det eit spesielt stort behov for å ha gode tryggings- og personverntiltak. Det offentlege administrerer mange svært omfattande register med personopplysningar, mellom anna registera til helse- og omsorgstenesta. For at ein skal kunne garantere tryggleiken og personvernet til dei registrerte, er det viktig å ha system på plass som kan skilje mellom ulike roller og tilgangsnivå, slik at dei rette personane får den tilgangen dei skal ha.

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. På fysiske legitimasjonsdokument blir personar gjerne identifiserte med namn og fødselsdato, eventuelt fødselsnummer. Eit fødselsnummer identifiserer ein person, medan det i kombinasjon med eitt eller fleire passord, PIN-kodar eller for eksempel eit personleg smartkort kan autentisere ein person. 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.

9.5.1 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 å bruke personlege brukarnamn og passord som kvar einskild får tildelt, og som han eller ho beheld i den autoriserte perioden. Dette går òg under namnet ein-faktor-autentisering, det vil seie at ein autentiserer seg ved bruk

[16] *Opinion 04/2012 on Cookie Consent Exemption (WP 194).*

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. Dette blir mellom anna gjort for å logge seg på ID-porten ved bruk av MinID, ei løysing svært mange bruker.

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. Dei private nøklane blir for eksempel utferda som smartkort eller USB-pinnar som inneheld ein elektronisk ID. Dei kan òg lagrast på nett, då blir det kalla nettsentrisk lagring av nøklar. Ein aktør som leverer løysingar baserte på PKI, er Buypass. Dei bruker smartkort til dei private nøklane til brukarane, og tilbyr mellom anna løysingar for trygg tilgang til Altinn og leverer tippekortløysingar til Norsk Tipping. I dag er mellom anna infrastrukturen for pass basert på PKI, for å verne fingeravtrykk og andletsbiometri som er lagra i passet. BankID er ein annan aktør som bruker denne teknologien. Ved bruk av BankID er dei private nøklane til brukarane lagra hos bankane. Infrastrukturen for pass bruker òg PKI-teknologien for å verne fingeravtrykk og andletsbiometri som er lagra i passet. 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 har fordelar framfor dei meir tradisjonelle autentiseringsmetodane som det er gjort greie for ovanfor. Eit mangfald av brukarnamn og passord kan ofte føre til auka risiko for misbruk ved at dei for eksempel kan skrivast ned og bli sedde av eller delte med andre. 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. Biometri kan òg nyttast berre til å autentisere, slik som å slå fast at det er same personen som autentiserer seg ved to ulike høve. For eksempel brukte SAS i ein periode fingeravtrykk ved innsjekking av bagasje og så igjen ved ombordstiging for å sjekke at det var den personen som hadde sjekka inn bagasje, som òg gjekk om bord i flyet. Personvernnemda har i løpet av 2012 kome med to avgjerder som opnar for utvida bruk av biometri der ein berre autentiserer og ikkje identifiserer[17].

9.5.2 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. Ein mellombels tilsett kan for eksempel ha svært avgrensa tilgang til enkelte delar av det konfidensielle fillageret til eit firma, men likevel ha behov for vid tilgang til data innanfor eit meir snevert område. Det motsette kan òg vere tilfelle, for eksempel når det er behov for å gi ein leiar vid tilgang til områda i eit IKT-system, men med viktige unntak for enkelte sensitive dokument som berre er tilgjengelege for dei tilsette på personalavdelinga.

Det er krevjande å lage dekkjande roller for tilgangsstyring i IKT-system. I enkelte sektorar, for eksempel helse- og omsorgssektoren, trengst det større tilgang i spesielle situasjonar, og ein må vege behovet for å sikre konfidensialitet opp mot behovet for å gi tilgang. Ei utfordring for dei som skal praktisere den tekniske identitetsforvaltinga, er å oppdatere systemet etter kvart som rollene og behovet for tilgang endrar seg. 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 er viktig at aktørar som bruker system for identitetsforvalting, nyttar metodar for tilgangsstyring som er sikre og effektive. Passordløysingar er enkle å bruke, men ikkje særleg sikre, ettersom ein ikkje har nokon garanti for at uautoriserte personar ikkje får kjennskap til innloggingsinformasjonen til ein som er autorisert. Bruk av passord er for eksempel sårbart for skuldersurfing, tastaturavlytting og liknande. Og der eigaren lagar sitt eige passord, kan ein risikere at passordet ikkje er sterkt nok. Dersom ein bruker digitale sertifikat, er terskelen truleg høgare for å kunne overdra dei til uvedkomande. Dersom ein skal oppnå tilfredsstillande og tilpassa tryggleik, bør det leggjast til rette for å bruke løysingar for

[17] Sjå PVN 2011-11 Visma Retail og PVN 2011-12 Fitness 24 Seven.

sikker e-ID framfor passordløysingar og liknande for å få tilgang til register som behandlar sensitive personopplysningar.

9.5.3 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*[18]. 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. Rammeverket definerer fire tryggleiksnivå. Alle løysingar på eit høgare nivå kan brukast på eit lågare tryggleiksnivå.

Offentlege verksemder må gjennomføre risiko- og sårbarheitsanalysar når dei etablerer nye elektroniske tenester, og når dei reviderer eksisterande tenester. Verksemda må då vurdere kva konsekvensar uheldige hendingar kan få for brukarane av tenesta, den offentlege verksemda sjølv og offentleg sektor som heilskap. Deretter må verksemda vurdere kor sannsynleg det er at konsekvensar dei har identifisert, kjem til å inntreffe. Kvar offentleg verksemd må derfor sjølv vurdere kva som er eit akseptabelt risikonivå, og kva tryggleiksnivå som gir god nok tryggleik for verksemda og brukarane.

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. Alle er personlege elektroniske ID-ar som ein kan bruke når ein loggar seg på tenester frå for eksempel arbeids- og velferdsetaten, Lånekassen, Utlendingsdirektoratet og skatteetaten.

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). Slike sertifikat blir i stor grad nytta for nettenester (SSL-sertifikat).

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. På den måten kan innsynet foreldra har i elev-lærar-forholdet avgrensast, sjølv om foreldra får innsyn i den kommunikasjonen som er viktigast for dei. Elevane kan på same måten skjermast for kommunikasjon mellom lærarane og foreldra der dette er føremålstenleg. Det er vidare mogleg å gi tilgang til berre éin forelder i tilfelle der den andre av ulike grunnar ikkje bør ha tilgang. Det at ein har opna for å gjere slike skjønsvurderingar, kan føre til at det blir teke betre omsyn til kvar enkelt elev og personvernet hans eller hennar.

9.5.4 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. Det inneber at leverandørane frivillig har erklært til tilsynet at dei oppfyller nærmare fastsette krav for å kunne skrive ut sertifikat på nivå 4. Ordninga er frivillig og medverkar til auka tillit til sertifikattenester. Det gir òg Post- og teletilsynet høve til å føre tilsyn med aktørane og krevje revisjon frå tredjepart.

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.

9.5.5 Sterkare grep om identitetsforvalting

Grunnidentifisering og registrering av norske borgarars identitet i offentlege register er eit

[18] Fornyings- og administrasjonsdepartementet: Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. Retningslinjer for offentlige virksomheter som tilrettelegger elektroniske tjenester og samhandling på nett. April 2008.

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. Til å identifisere seg i det daglege bruker ein som oftast førarkort eller bankkort, sidan passet ikkje høver til dagleg bruk.

Dette er noko av bakgrunnen for at regjeringa no arbeider med ei løysing for nasjonalt ID-kort med e-ID i Noreg. Nasjonalt ID-kort skal knytast til utferding av pass, både organisatorisk og teknisk. Det vil derfor ha same graden av tryggleik som passet, ved at det blir utferda av politiet og krev personleg oppmøte. 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.

9.6 Innsynslogging

Ein effektiv måte å unngå at uvedkomande får innsyn og «snokar» i opplysningar dei ikkje har behov for å sjå, er å loggføre kvar enkelt sin bruk av systemet. 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. Med logging meiner regjeringa i denne samanhengen innsynslogging, slik det er presentert i kapittel 9.3.2. Behandlingsansvarlege har allereie ei generell plikt til å utføre nettverksbasert logging etter personopplysningslova § 13.

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. Ein kan for eksempel tenkje seg at dei som har leiarroller med mykje ansvar, bør ha vidare tilgang enn andre. Slik vid tilgang kan kombinerast med å stille leiarar til ansvar dersom dei misbruker denne tilgangen.

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. Dersom ein for eksempel har klåre grenser for kor mange personar som kan ha tilgang, blir den som tildeler roller med tilgang, òg meir restriktiv i tildelinga. Slike klåre grenser kan setjast gjennom veldefinerte parametrar for tilgang i eit system. Slike parametrar må òg vere rettleiande for logginga og kva hendingar som bør få det til å ringje ei varselbjølle. 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. Dette vil særleg kunne skje dersom det er eksterne aktørar eller nokon som ikkje kjenner til lokale forhold hos den aktuelle behandlingsansvarlege, som les av 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. Det er mange tenkjelege situasjonar der det kan vere gode grunnar for ei handling som er loggført som mistenkjeleg, og dei faktiske forholda vil tilseie at handlinga var reglementert. 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. For det første er det nødvendig å loggføre kven som får innsyn og når, og dessutan mislukka forsøk på innsyn. Det kan òg

vere føremålstenleg å loggføre kvar det blir oppnådd innsyn, kor lenge vedkomande hadde innsyn, og eventuelt kva søkjeord som er brukt for å finne det aktuelle dokumentet. Det blir utvikla stadig fleire program for såkalla «flagging» av bruksmønster som kan indikere mogleg snoking. Søkjemønsteret til ein brukar og korleis vedkomande bruker informasjonssystemet, kan bli flagga dersom bruken endrar seg merkbart. Dette må deretter følgjast opp av personell som er ansvarleg for å gå gjennom loggar, og eventuelt av den overordna til den aktuelle brukaren. Slike flaggingssystem kan, dersom dei blir implementerte på rett måte, medverke til at innsynsloggar blir handterte på ein betre og meir effektiv måte.

I helse- og omsorgssektoren har ein eigne reglar for innsynslogging og innsyn i loggar. Pasientar har fått rett til innsyn i eigen journal og i loggar frå behandlingsretta register etter pasientrettslova § 5-1 og helseregisterlova § 13 sjette leddet. Dei nærmare krava til innsynslogginga i helseregistera er fastsette i helseinformasjonstryggingsforskrifta[19] § 16. Det er for tida arbeid i gang med prosjekt i helse- og omsorgssektoren for korleis program for attkjenning av mønster kan medverke til meir effektiv gjennomgang av loggar. Dette er eit krevjande arbeid, særleg på grunn av den store mengda av opplysningar som blir behandla, og dei mange rollene som ligg i IKT-systema i helse- og omsorgssektoren. Det er òg viktig å ta omsyn til det særlege behovet som helsepersonell kan ha for tilgang til helseopplysningar i nødssituasjonar. Sjølv om arbeidet med effektiv logging er krevjande, er det likevel eit svært viktig arbeid. Dette er noko som bør gjerast i alle sektorar med større register.

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

Det at den registrerte skal få innsyn i eigne personopplysningar, er eit viktig personvernprinsipp. Innsynet blir mellom anna grunngitt med at ein gjerne har interesse av å kontrollere kva opplysningar andre har om ein sjølv, og interesse av å kunne be om å få opplysningar retta eller sletta. Etter personopplysningslova § 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 er viktig at kvar einskild blir informert om retten til å få innsyn i innsynsloggane til dei registera der han eller ho er oppført. Viss informasjonen som blir gitt til dei registrerte om innsynsretten, ikkje er god, kan denne retten til innsyn i loggar raskt bli ein rett som det er vanskeleg å praktisere. Det er derfor spesielt viktig for dei behandlingsansvarlege som lagrar sensitive personopplysningar, for eksempel sjukehus og legekontor, å gi god informasjon om innsynsretten.

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. Ein må kunne vite heilt sikkert at den som har hatt innsyn i opplysningane, faktisk er den personen som har fått tilgang. Det er viktig at påloggingsrutinane for dei ulike registera og systema er gode og sikre, og at metodane for identifisering/autentisering er best mogleg. Dersom systema for identitetsforvalting ikkje er gode nok, blir heller ikkje systema for logging gode nok.

Vidare må ein 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 kan tenkjast at omfanget av innsyn i loggar bør variere noko frå register til register. I somme register kan det vere behov for eit noko avgrensa innsyn av omsyn til integritet eller sikring av personvernet til andre. For andre loggar kan det vere nødvendig å praktisere ein noko utvida innsynsrett. 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.

9.6.2 Logging i større offentlege og private register

Logging er spesielt viktig i dei store registera der ein behandlar sensitive personopplysningar. Nedanfor 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. Føremålet med lagringa er å avdekkje tryggleiksbrot og urettkomen behandling av personopplysningar.

[19] Forskrift av 24. juni 2011 om informasjonssikkerhet ved elektronisk tilgang til helseopplysninger i behandlingsrettede helseregistre.

I samband med avgjerda om å modernisere arbeids- og velferdsetaten er det sett i gang ei omfattande modernisering av datasystema til etaten. Her skal det mellom anna utviklast meir moderne system for tilgangskontroll. Etaten har allereie etablert system for logging i samsvar med føresegnene om informasjonstryggleik i personopplysningsforskrifta. Datatilsynet har derimot påpeikt, etter at dei i november 2010 gjennomførte kontrollar ved utvalde Nav-kontor[20], at sikringa av fortrulegskap gjennom tilgangsstyring og logging ikkje er god nok. Det gjekk mellom anna fram av kontrollrapporten at innsynslogging ikkje var implementert i alle fagsystema som er i bruk i arbeids- og velferdsetaten. Vidare uttala Datatilsynet at den manglande gjennomgangen av loggane var uheldig. Hovudutfordringane med dagens system er knytte til etablering og oppfølging av dei etablerte loggane, sikring av tilfredsstillande tilgangskontroll i datasystema til etaten og forankring av eit godt styringssystem for informasjonstryggleik. Som ein del av moderniseringsarbeidet må dei gå gjennom dei eksisterande rutinane for innsynslogging og vurdere om det er nødvendig å gjere endringar i dei. 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. Dei nye konsesjonsvilkåra tok i utgangspunktet til å gjelde 1. januar 2011. 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. Fleire norske bankar samarbeider no med Finansnæringens Fellesorganisasjon (FNO) for å oppfylle dei nye vilkåra innan implementeringsfristen. Forsikringsverksemder har eigen konsesjon frå Datatilsynet. Konsesjonsvilkåra stiller ikkje noko krav om at forsikringsverksemder skal praktisere logging av oppslag, og dermed heller ikkje om at kundane skal få noko innsyn i slike loggar. Forsikringsselskap behandlar mange og sensitive opplysningar om kundane sine, og dei har svært omfattande register. Dette gjeld særleg på området for livsforsikringar. Ein bør vurdere om det bør stillast liknande vilkår om logging og utvida innsyn til forsikringsverksemder som til finansverksemder.

[20] Datatilsynets endelige kontrollrapport fra tilsyn hos Arbeids- og velferdsdirektoratet og Nav kontaktsenter i Bodø. Rapport 10/01228, datert 6. mai 2011.

9.6.3 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.

Det finst generelt lite informasjon om korleis innsynslogging blir praktisert i dei ulike større registera. Dette kjem i stor grad av at det er opp til kvar enkelt verksemd å bestemme rutinane for logging og korleis loggane skal verifiserast. Det finst ingen sentrale retningsliner for korleis dette skal gjerast i kvar einskild sektor. 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.

9.7 Samandrag og tilrådingar

Den generelle auken i bruk av internett og sosiale medium og utviklinga av avanserte metodar for lagring og sporing fører med seg nye og viktige problemstillingar knytte til personvernet. Det teknologiske landskapet er prega av at endring er den einaste konstanten. Dersom ein ikkje tek mål av seg til å møte utviklinga av ny teknologi i framtidig personvernregulering, kan det få konsekvensar for personvernet. Det overordna målet i dette kapittelet har derfor vore å understreke kor viktig det er med innebygd personvern. Ikkje berre i lovgivingsprosessane, men òg i prosessane der det blir utvikla og implementert ny teknologi, må ein krevje at personvernet blir sikra på ein god måte.

Det offentlege har ansvar for å gå føre med eit godt eksempel når det gjeld implementering av godt personvern. Dette blir gjort både ved at personvern blir bygd inn i offentlege løysingar, og ved at offentlege styremakter arbeider godt og målretta for å opplyse innbyggjarane og dei private aktørane om personvern. Ein bør derfor fastsetje eit prinsipielt mål om innebygd personvern i alle sektorar. For å oppnå dette er det spesielt viktig å stille krav i dei ulike sektorane, eksempelvis gjennom bransjenormer, om at dei mest personvernvenlege løysingane skal byggjast inn i utstyr, system og programvare som førehandsdefinerte standardinnstillingar.

Blant dei viktigaste nye teknologiane som opnar for betre effektivitet og tryggleik, er nettskyteknologien og bruken av biometri. Teknologiane inneber likevel visse utfordringar for personvernet. Regjeringa ønskjer å leggje til rette for sikker og forutsigbar bruk av nettskytenester innanfor rammene av det norske regelverket, blant anna ved å utarbeide rettleiingar. Når det gjeld biometri, ser regjeringa at det trengst ein brei diskusjon rundt kva typar føremål det er ønskjeleg å bruke desse teknologiane til.

Ein annan tendens i den teknologiske utviklinga er at ny teknologi i stadig større grad gjer det mogleg med elektronisk sporing av enkeltpersonar. Det kan for eksempel dreie seg om lokaliseringstenester på smarttelefonar, sporing av bilar, sporing av internettsøk eller lagring av informasjonskapslar til ulike føremål. Regjeringa meiner at det skal leggjast til rette for å bruke anonyme alternativ for dei som ønskjer det, og bruken av slike alternativ skal ikkje innebere noka ulempe for dei som vel dei. Det er dessutan viktig å presisere at der det er påkravd med samtykke til bruk av sporingsteknologi, bør ein unngå tekniske løysingar for innhenting av samtykke som grensar mot implisitt samtykke eller ei form for reservasjonsrett.

Identitetsforvalting og tilgangsstyring er viktige verkemiddel for å sikre personvernet til dei som er registrerte i større register. Det er svært viktig å sikre at rett person får tilgang til dei rette opplysningane til rett tid. Dette føreset gode løysingar for å identifisere og autentisere dei personane som er autoriserte for tilgang i registera. Eit mål må vere å innføre sikker e-ID for tilgang der dette er mogleg.

For å sikre at identitetsforvaltinga i IKT-system fungerer som ho skal, må plikta til klientbasert logging og retten til innsyn i eigne loggar vere eit berande prinsipp for alle større offentlege og private register. Ettersom ein per i dag ikkje har noka god oversikt over korleis logging og innsyn i loggar blir praktisert i dei ulike registera, er det behov for å undersøkje dette nærmare.

Boks 9.1 Hovudpunkt kapittel 9

- 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.

10 Personvernstyremakta – organisering og oppgåver

10.1 Innleiing – oppgåver og verkemiddel, status i andre land

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. Her heiter det:

Datatilsynet skal:

1) føre en systematisk og offentlig fortegnelse over alle behandlinger som er innmeldt etter § 31 eller gitt konsesjon etter § 33, med opplysninger som nevnt i § 18 første ledd jf. § 23,
2) behandle søknader om konsesjoner, motta meldinger og vurdere om det skal gis pålegg der loven gir hjemmel for dette,
3) kontrollere at lover og forskrifter som gjelder for behandling av personopplysninger blir fulgt, og at feil eller mangler blir rettet,
4) holde seg orientert om og informere om den generelle nasjonale og internasjonale utviklingen i behandlingen av personopplysninger og om de problemer som knytter seg til slik behandling,
5) identifisere farer for personvernet, og gi råd om hvordan de kan unngås eller begrenses,
6) gi råd og veiledning i spørsmål om personvern og sikring av personopplysninger til dem som planlegger å behandle personopplysninger eller utvikle systemer for slik behandling, herunder bistå i utarbeidelsen av bransjevise atferdsnormer,
7) etter henvendelse eller av eget tiltak gi uttalelse i spørsmål om behandling av personopplysninger, og
8) gi Kongen årsmelding om sin virksomhet.

Datatilsynet fører i tillegg tilsyn etter mellom anna helseregisterlova og helseforskingslova og vil få tilsynsoppgåver etter politiregisterlova og ekomlova (implementering av datalagringsdirektivet) når desse lovverka blir sette i kraft.

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.

Oppgåvene som er fastsette i personopplysningslova, fastset òg langt på veg kva verkemiddel tilsynet kan nytte i arbeidet. 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* strekar under at Datatilsynet er unnateke frå den alminnelege instruksjonsmyndigheita som ligg til Justisdepartementet[1] i eigenskap av overordna organ. Utvalet som utarbeidde NOUen meinte vidare at departementet har instruksjonsmyndigheit når det gjeld organisatoriske og administrative forhold, og at departementet i budsjettbehandlinga kan «sette mål og veilede i tråd med gjeldende lover og regler og retningslinjer for oppfølging av underliggende virksomheter». Utvalet understreka at måla vil vere av generell karakter, medan den meir «detaljpregede, fortløpende planleggingen og prioriteringen forestås av tilsynet selv». Utvalet peikte på at «departementets

[1] Datatilsynet er no underlagt Fornyings-, administrasjons- og kyrkjedepartementet.

etatsstyring må ta hensyn til at tilsynsmyndigheten skal være faglig uavhengig».

At Datatilsynet skal vere uavhengig, er stadfesta i Ot. prp. nr. 92 (1998-99) og i Innst. O. nr 51 (1990–2000), der «komiteen er enig med Justisdepartementets 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. Dette er det gjort nærmare greie for i artikkel 47, der det mellom anna heiter at den uavhengige stillinga til styremakta skal vere fullstendig («complete») når ho utøver oppgåvene og myndigheita si. 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. Personvernarbeidet desse styremaktene gjer, er ikkje nærmare omtala i meldinga, men meldinga vil i punkt 10.4, 10.5.4 og 10.5.9 kome inn på det samarbeidet Datatilsynet har med eksterne aktørar for å styrkje den sektorvise personvernkompetansen.

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. Av dei nordiske tilsynsstyremaktene er det den svenske Datainspektionen som liknar mest på det norske Datatilsynet. Datainspektionen har i hovudsak oppgåver som samsvarar med oppgåvene den norske personvernstyremakta har, og er om lag like stor som det norske Datatilsynet. På same måten som Datatilsynet skal Datainspektionen behandle saker og føre tilsyn med at personvernregelverket blir etterlevd, og spreie kunnskap, vekkje debatt og åtvare om trugsmål mot personvernet. Det finske datatilsynet, Dataombudsmannens byrå, skal òg vekkje debatt og spreie kunnskap i tillegg til å føre tilsyn med at personvernregelverket blir etterlevd. Dataombudsmannens byrå er derimot ein liten organisasjon med berre 20 tilsette, og aktivitetsnivået er noko avgrensa på grunn av det. Det danske Datatilsynet har ei mindre utprega ombodsrolle enn dei nordiske systerorganisasjonane sine. 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.

10.2 Hovudmoment i rapporten frå Personvernkommisjonen

Organiseringa av personvernstyremakta er omtala i kapittel 11 i rapporten frå Personvernkommisjonen. Kommisjonen går gjennom den rettslege forankringa, leiinga, arbeidsoppgåvene, budsjettet og bemanninga til Datatilsynet. Vidare drøftar kommisjonen rollene til Datatilsynet som ombod og tilsyn og omgjering av vedtak i Personvernnemnda. Personvernkommisjonen kjem med fleire forslag til endringar. Forslaga er drøfta i punkt 10.5 nedanfor og omhandlar desse temaa:

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

10.3 Hovudfunn i evalueringa til Difi

I dei drygt 30 åra Datatilsynet har eksistert, har det ikkje vore gjennomført noka evaluering med tanke på å kartleggje om etaten har dei nødvendige ressursane og føresetnadene for å kunne fylle rollene og oppgåvene sine slik det er føresett i personopplysningslova. Hausten 2010 gav derfor 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[2] vart framlagd 3. oktober 2011.

Det var brei semje blant informantane om at Datatilsynet oppnår gode resultat med etter måten små ressursar. Det vart særleg peikt på at Datatilsynet er synleg i media og har god evne til å setje personvernspørsmål på saklista. Datatilsynet fekk òg stort sett positiv tilbakemelding på utøvinga av myndigheit, men ein viss kritikk for rolleforståinga.

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 Justisdepartementet 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.

10.4 Datatilsynet – den nye arbeidsforma og den meir strategiske tilnærminga

Datatilsynet manøvrerer i eit krevjande landskap med kryssande interesser. Rollene som både tilsyn og ombod krev god evne til å manøvrere i dette landskapet. For å leggje til rette for effektiv ressursbruk på alle område gjennomførte Datatilsynet ein intern strategiprosess parallelt med evalueringa til Difi. Den nye strategien[3] 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. Heile organisasjonen deltek i arbeidet med planen. På månadlege møte blir det rapportert om framdrifta. I desse møta blir òg restansar i saksbehandling og tilsyn gjennomgått. I tillegg har Datatilsynet vedteke fagstrategiar på helseområdet, i justissektoren og på det internasjonale området. Slike strategiar er nyttige styringsverktøy internt, samtidig som dei gir omverda viktig informasjon om grunnlaget for arbeidet Datatilsynet gjer med personvern i den sektoren strategien gjeld for.

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. Eit sentralt verkemiddel er det å ha brei kontakt med viktige aktørar i næringsliv, politikk, offentleg forvaltning og ulike forskings- og utviklingsmiljø.

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.

10.5 Datatilsynet framover

10.5.1 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 spørs-

[2] Rapport frå Difi 2011:8

[3] Datatilsynet sin strategi 2011–2016, datert 11. november 2011.

mål. 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. Det kan oppstå situasjonar der Datatilsynet som ombod kritiserer ei avgjerd eller eit selskap som dei seinare skal føre tilsyn med. Dette peikte òg Difi på i rapporten sin. Ein måte å takle denne utfordringa på kan vere å opprette eit reint personvernombod som einast skal ta hand om personvernet, slik eit mindretal på éin medlem i Personvernkommisjonen gjekk inn for.

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. Somme av informantane i evalueringsmaterialet til Difi peiker òg på at Datatilsynet til tider ter seg meir som ein politisk aktør enn som eit forvaltningsorgan. Dette *kan* vere eit uttrykk for ei uklår rolleforståing, og at ombodsrolla blir trekt for langt inn i saksbehandlinga. Datatilsynet har dei seinare åra sett kor viktig det er å ha god rolleforståing og vere tydeleg i utøvinga av rollene. 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. Dette er særleg viktig i eit samfunn der den teknologiske utviklinga går svært raskt. Datatilsynet har for eksempel hatt omfattande dialog med Facebook og Google og har arbeidd for å påverke desse selskapa til å betre forretningspraksisen sin og gi betre informasjon til brukarane. Sjølv om det er usikkert kor langt den formelle jurisdiksjonen strekkjer seg i denne dialogen, gjer ombodsrolla det mogleg å føre ein slik dialog utan å vere bunden av formelle skrankar.

Aktivt internasjonalt engasjement er viktig for Datatilsynet. Det er bygd opp eit omfattande samarbeid mellom datatilsynsstyremakter i Europa. Dette samarbeidet blir ytterlegare styrkt dersom forslaget til ny forordning om personvern i EU blir vedteke. Eit eventuelt reint ombod på personvernområdet vil ikkje ha tilgang til dette nettverket.

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. Dette kan derimot avhjelpast ved at etaten tydeleg forankrar tilsynsverksemda si i det gjeldande regelverket, både forvaltningsrettsleg og personvernrettsleg.

I Datatilsynet sitt tilfellet 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.

10.5.2 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 strekar under at dette er viktig arbeid. I eit stadig meir teknologidrive samfunn der utviklinga går svært fort, er det viktig at arbeidet til forvaltninga i størst mogleg grad er basert på kunnskap. Dette gjeld kanskje særleg på eit område som personvern, som grip inn i nær sagt alle samfunnsområde og krev breie analysar og samansette avvegingar. Ved å ha kontakt med FoU-miljøa får Datatilsynet eit betre kunnskapsfundament til å utøve både tilsyns- og ombodsrolla. FoU-miljøa vil ha nytte av den praktiske erfaringa Datatilsynet opparbeider seg gjennom tilsyn, saksbehandling og rettleiingsarbeid. Regjeringa legg derfor til grunn at Datatilsynet held fram med å utvikle forholdet til forskings- og utviklingsmiljøa til felles nytte.

10.5.3 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.

Datatilsynet hadde fram til 2000 eit styre med sju medlemer, som primært behandla klagesaker, saker som aktualiserte nye eller endra problemstillingar for personvernet, og saker som gjaldt sentrale samfunnsspørsmål. Styret var breitt samansett, med mellom anna interesserepresentasjon frå partane i arbeidslivet, og skulle gjere breie avvegingar av ulike omsyn. Styret vart avvikla og erstatta av Personvernnemnda då personopplysningslova vart sett i kraft 1. januar 2001.

Det er ikkje 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. Eit råd vil vere partssamansett og vil òg ha medlemer frå næringar eller interesseorganisasjonar som avgjerdene til Datatilsynet får direkte følgjer for. Eit råd kan derfor kunne rokke ved den uavhengige stillinga til Datatilsynet.

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. På same måten som det tidlegare styret er òg Personvernnemnda breitt samansett med ulik kompetanse for nettopp å kunne vurdere personvern opp mot andre sentrale samfunnsinteresser. Desse vurderingane gjer nemnda på ein god måte.

10.5.4 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. I punkt 7.10 i rapporten skriv Difi at det vil vere «verdt å vurdere hvordan Datatilsynet kan komme i enda bedre inngripen med andre statlige tilsyn slik at personvern blir ivaretatt på lik linje med andre hensyn både i offentlig og privat virksomhet». Personvernkommisjonen peiker i punkt 18.3.6 på at samarbeidet med eksterne aktørar bør halde fram, og viser mellom anna til suksessen med undervisningskampanjen *Du bestemmer*, som Datatilsynet, Teknologirådet og Senter for IKT i utdanninga samarbeider om.

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. Mange eksterne aktørar har behov for å få betre kjennskap til personvern og korleis personvernomsyn kan takast vare på. Gjennom aktiv rådgiving kan Datatilsynet bidra til at desse aktørane 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. Datatilsynet skal ikkje førehandsgodkjenne bestemte løysingar og må sørgje for å gjere dei tiltaka som trengst for å sikre handlingsrommet i eventuelle klagesaker.

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 avveigingane feltet krev.

10.5.5 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.

Gjennom Digitaliseringsprogrammet har regjeringa eit klårt mål om at elektronisk kommunikasjon skal vere den primære plattforma for dialogen mellom innbyggjarane/næringslivet og det offentlege. Ei god heimeside er ein føresetnad for å oppfylle målet regjeringa har sett seg. Heimesida vil gjere brukarane i stand til i stor grad å hjelpe seg sjølve. Brukt på rett måte kan heimesida òg heve servicenivået ved å gi god informasjon på nett.

Det er ikkje grunn til å tru at saksmengda til Datatilsynet kjem til å bli mindre i åra framover. Det er derfor viktig at tilsynet stadig arbeider for å effektivisere arbeidsmetodane sine. Personvernområdet er svært breitt, og det er viktig å gjere dei rette prioriteringane og bruke dei rette verkemidla for å nå målet om best mogleg personvern for innbyggjarane.

10.5.6 Kompetansen til Datatilsynet

Både Personvernkommisjonen og Difi understrekar at det er viktig at Datatilsynet har ein breitt samansett kompetanse. Personvernkommisjonen føreslår (i punkt 18.3.2 i rapporten) at Datatilsynet spesielt bør styrkje den tekniske kompetansen ved nytilsetjingar, og trekkjer særskilt fram behovet for kompetanse på personvernfremjande teknologi, identitetsforvaltning, nye medium og design av informasjonssystem. Difi på si side (punkt 7.8 i rapporten) understrekar at Datatilsynet har god teknologikompetanse og god sektorkompetanse men meiner at forvaltningskompetansen til tilsynet bør styrkjast.

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. Dette kan dei mellom anna opparbeide gjennom å ha god kontakt med dei ulike sektorane og andre tilsynsstyremakter. Regjeringa har som mål å digitalisere offentlege tenester. Dette skaper utfordringar, men òg gode utsikter for personvernet. 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. Den internasjonale utviklinga er òg svært viktig på personvernområdet, jamfør kapittel 3. God internasjonal kompetanse gjer det lettare å få gjennomslag i internasjonale forum, og derfor blir òg slik kompetanse vurdert som spesielt viktig.

10.5.7 Regionalisering av Datatilsynet

Personvernkommisjonen meiner Datatilsynet bør regionaliserast, og føreslår å opprette fleire regionkontor. Føremålet er å få ei meir lokal forankring i personvernarbeidet. Kommisjonen meiner lokal tilknyting vil tilføre viktige perspektiv når ein vurderer om overvakingstiltak er føremålstenlege, og når ein vel ut tilsynsobjekt. Liknande forslag har òg vore fremja tidlegare, mellom anna eit forslag om å gi kommunane ansvaret for å behandle søknader om løyve til å drive kameraovervaking. Slik regjeringa forstår kommisjonen, er forslaget om regionalisering knytt til det generelle forslaget om å styrkje Datatilsynet slik at veksten bør kome i regionane.

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. Dette kan ikkje forsvarast når samfunnsutviklinga går i retning av stadig meir press på personvernet og tilsvarande behov for eit tydeleg og sterkt tilsyn. Heller ikkje dei nor-

diske nabolanda våre har valt å regionalisere personvernstyremakta. Det kan tyde på at heller ikkje dei har sett eit stort behov for å ha eit regionapparat på personvernområdet. 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. Ressursbehovet til etaten dei komande åra blir omtala nedanfor.

10.5.8 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.

Datatilsynet har i dag 40 tilsette. Til samanlikning har den svenske datatilsynsstyremakta omtrent like mange tilsette og eit budsjett som er ca. kr 3 mill. høgare enn budsjettet til Datatilsynet. Det danske Datatilsynet har drygt 30 tilsette og eit budsjett på ca. 20 millionar danske kroner. Det norske Datatilsynet har slik sett fleire tilsette i høve til folketalet enn dei andre nordiske datatilsyna. Og 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 millionar kroner i høve til 2012-budsjettet for å setje tilsynet i stand til å ta seg av desse oppgåvene.

Regjeringa registrerer at Personvernkommisjonen i rapporten sin tilrådde å styrkje tilsynsstyremakta, og at dette spesielt bør skje i form av styrkt teknologikompetanse, med fokus på identitetsforvalting, digitale medium og informasjonstryggleik. Regjeringa vil vurdere frå år til år om og eventuelt kor mykje budsjettet skal aukast. Det er ikkje vanleg med øyremerking av budsjettmidlane til Datatilsynet, og regjeringa meiner det mest føremålstenlege er at Datatilsynet også i framtida sjølv vurderer kva kompetanse etaten til kvar tid har bruk for.

10.5.9 Sektorvis styrking av personvernkompetansen

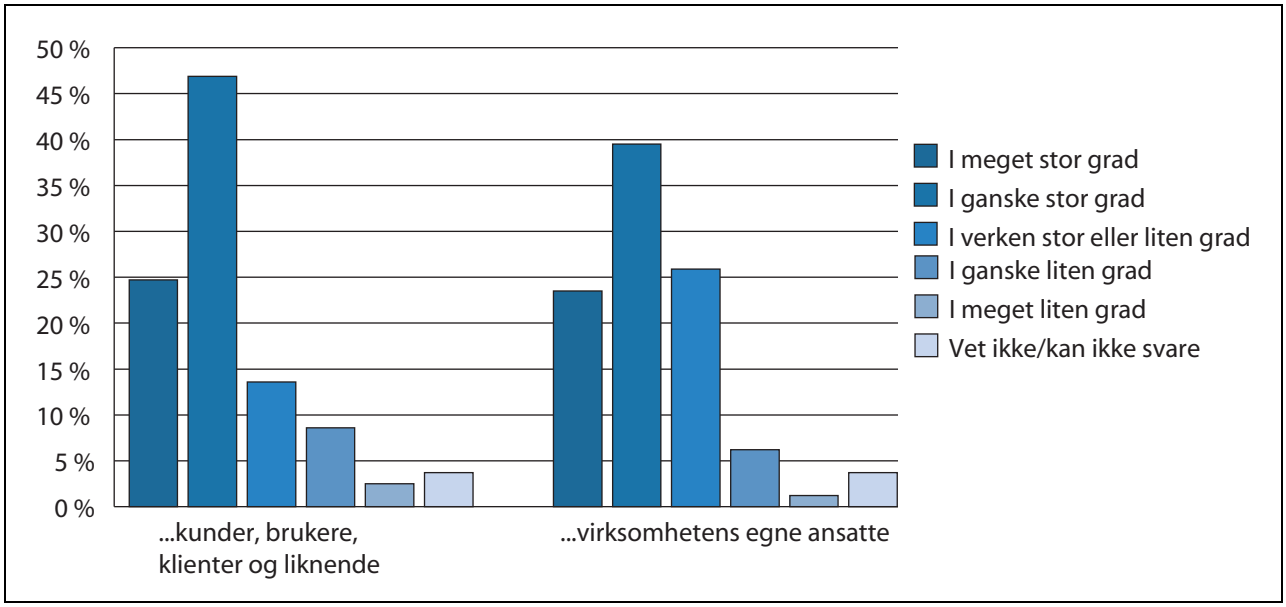
Personvernkommisjonen føreslår å styrkje personvernkompetansen sektorvis ved at andre organ som får med personvernspørsmål å gjere, bør ha ein person internt med høg kompetanse på personvernspørsmål. Det er føreslått at dette først og fremst blir gjort gjennom å opprette personvernombod i desse organa.

Regjeringa er einig med kommisjonen i at organ som ofte har med personvernspørsmål å gjere, bør ha spesiell kompetanse på området. Ei rekkje organ, til dømes i helsesektoren og ein del kommunar, har oppretta personvernombod. I politiregisterlova er det dessutan innført ei obligatorisk ordning med personvernrådgivarar i politiet.

Regjeringa vil sjå spørsmålet om sektorvis styrking av personvernet i samanheng med utviklinga av personvernombodsordninga, sjå kapittel 10.6 nedanfor. 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. 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.

10.6 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. Nokre av omboda har så mange oppdragsgivarar at ein kan spørje seg om dei har



Figur 10.1 Rapport: Evaluering av personvernombudsordningen 2011

Kilde: Synnovate/Ipsos MMI

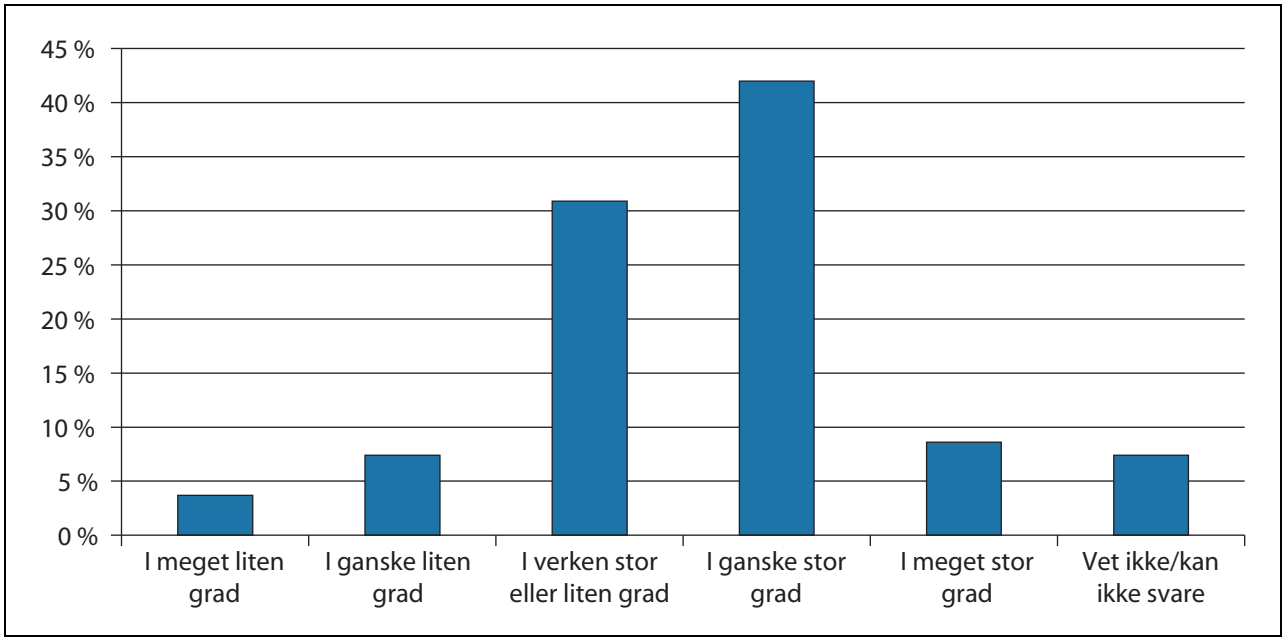
reell oversikt over alle behandlingane av personopplysningar som skjer, og om dei kan hjelpe både dei behandlingsansvarlege og dei registrerte på den måten som er ønskt og føresett. Andre personvernombod er tilsette i verksemda og har oppgåva som personvernombod på fulltid. Dei blir omtala som personvernombod, 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 Justisdepartementet 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 for den behandlingsansvarlege og få ein negativ innverknad på personvernet til dei registrerte. 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»), sjå artikkel 35 og utover i forslaget. Det er føreslått å gi ombodet mange oppgåver, mellom anna å informere behandlingsansvarlege om dei reglane som gjeld for behandling av personopplysningar, sørgje for at det blir implementert god internkontroll, og ha kontakt med datatilsynsstyremakta.

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. Eit stort fleirtal av dei spurde synest personvernomboda er nyttige. Leiinga i verksemdene er gjennomgåande meir positiv enn dei tilsette og omboda sjølve. Likevel meiner fleire av dei spurde i verksemdene at omboda ikkje styrkjer personvernet i verksemda nemneverdig.

Meiner dei behandlingsansvarlege at omboda medverkar til å styrkje personvernet for dei tilsette i verksemda og for eksterne kontaktar? Se figur 10.1.



Figur 10.2 Rapport: Evaluering av personvernombudsordningen 2011

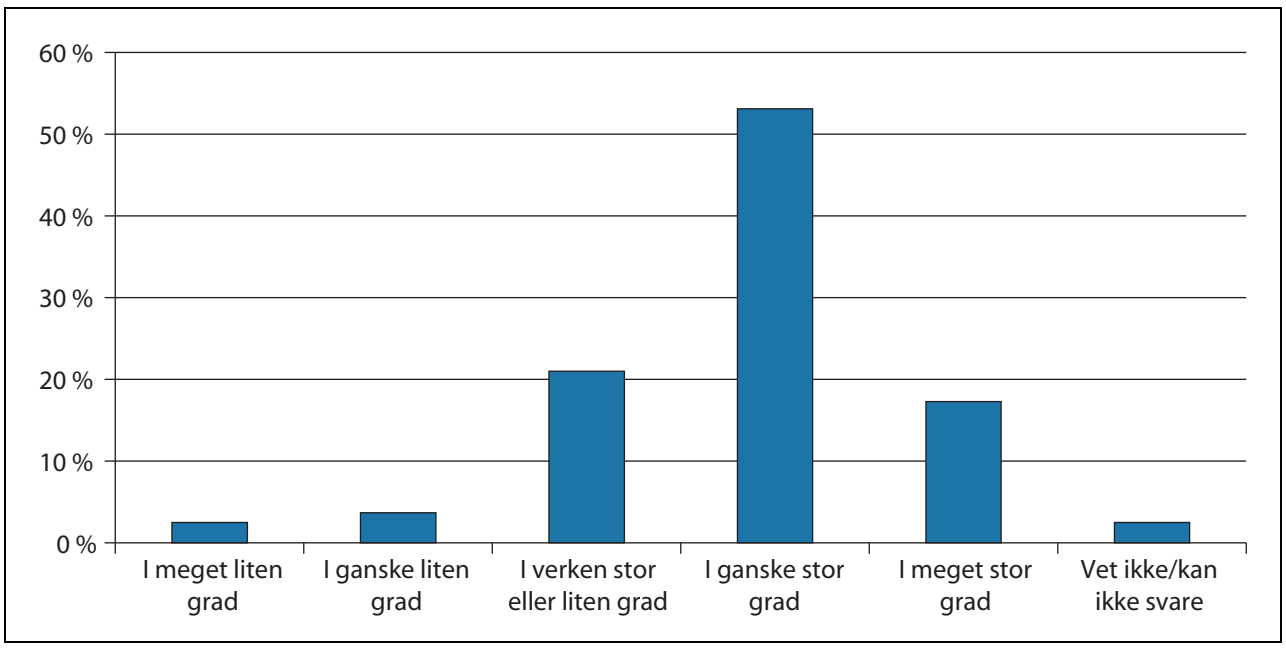
Kilde: Synnovate/Ipsos MMI

70 prosent av dei spurde meiner at etablering av personvernombod har skapt større medvit og kunnskap om personvern i verksemda. Samtidig meiner berre drygt halvparten at den faktiske regeletterlevinga har vorte betre.

I kva grad har regeletterlevinga auka i verksemda etter at det vart oppretta personvernombod? Se figur 10.2.

I kva grad har kunnskap og medvit om personvernregelverket auka i verksemda etter at det vart oppretta personvernombod? Se figur 10.3.

I periodar har Datatilsynet lagt mykje ressursar i å utarbeide rettleiingsmateriell for omboda og gi dei støtte og hjelp i arbeidet. Drygt 80 prosent av omboda svarar at dei er fornøgde med den faglege hjelpa dei får frå Datatilsynet. Omboda i



Figur 10.3 Rapport: Evaluering av personvernombudsordningen 2011

Kilde: Synnovate/Ipsos MMI

offentleg sektor er noko meir fornøgde enn dei i privat sektor.

I Difi-evalueringa av Datatilsynet vart det òg stilt spørsmål om ordninga med personvernombod. Svara i undersøkinga Difi har gjort, er med på å underbyggje dei noko sprikande svara om effekten av ordninga som kom fram i undersøkinga Synnovate utførte. Fleire ombod gav uttrykk for at dei synest det var vanskeleg å vite korleis dei skulle utøve rolla, og at dei opplevde manglande gjennomslag og forståing hos leiinga i verksemda. Somme gav òg uttrykk for at det er for sterkt fokus på dei positive sidene ved å etablere ombod, slik at enkelte verksemder kan ha vorte «lokka» til å innføre ordninga.

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. Dette er nødvendig for å sikre at oppgåver, rettar og plikter for alle som ordninga er aktuell for, er klårt definerte.

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 setje fokus på personvern i verksemda og på den måten styrkje regeletterlevinga. Rådgivaren kan gjere sitt til å betre personvernet for dei registrerte. Regjeringa vurderer det likevel som lite føremålstenleg å setje i gang eit arbeid med særnorsk regulering av ordninga med personvernombod no. Konsekvensen av det kan bli at ein må gjere endringar i ordninga etter relativt kort tid, når EU vedtek nye EØS-relevante reglar på området. Det kan bli både kostbart og krevjande for verksemder som nyleg har etablert personvernombod etter særnorsk ordning, å måtte tilpasse seg til nye krav i samsvar med reglar frå EU. Regjeringa ønskjer derfor 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.

10.7 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. Alle blir utnemnde for fire år om gongen med høve for å bli utnemnde på ny. Kompetansen til å utnemne medlemer er delt mellom Stortinget, som utnemner leiaren og nestleiaren, og regjeringa, som utnemner dei andre fem medlemene.

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.

Tabell 10.1 Tal på klagesaker mottekne i Personvernnemnda 2005–2011

2005	17 saker
2006	11 saker
2007	7 saker
2008	6 saker
2009	25 saker
2010	13 saker
2011	13 saker

Saksmengda i Personvernnemnda har variert noko sidan nemnda vart oppretta, men har dei seinaste åra lege på om lag 10–15 saker per år. Se tabell 10.1.

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 prosent av vedtaka i Datatilsynet blir sende inn til Personvernnemnda til klagesaksbehandling. Se tabell 10.2.

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, fungerer godt. Regjeringa har vurdert om det er grunnlag for å endre ordninga med personlege varamedlemer. Å ha varamedlemer utan personleg tilknyting til ein bestemt medlem kunne føre til at det oftare er dei same varamedlemene som deltek på møta i nemnda, og dermed til større kontinuitet i arbeidet. Ordninga i dag, der varamedlemene har kompetanse som langt på veg tilsvarar kompetansen til dei faste medlemene, blir likevel vurdert som god, ettersom ho sikrar at nemnda alltid er samansett av ulike typar kompetanse. Regjeringa vurderer det derfor inntil vidare som føremålstenleg å halde Personvernnemnda ved lag med personlege varamedlemer i den noverande forma.

10.8 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 personopplysningslova 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. Justis- og beredskapsdepartementet har etatsstyringsansvar for fleire offentlege verksemder som behandlar personopplysningar, mellom anna i justissektoren og tidlegare òg Brønnøysundregistra. Det administrative ansvaret for Datatilsynet vart flytt til Arbeids- og administrasjonsdepartementet i 2000 for å sikre at etatsstyringa av Datatilsynet ikkje

Tabell 10.2 Klageomfang i 2011

	Resultat 2011
Tal på vedtak gjorde av Datatilsynet	396
Tal på klager på vedtak	25
Tal på omgjeringar i Datatilsynet	3
Tal på oversendingar til Personvernnemnda	13

Det finst tal berre for 2011. Tala er baserte på manuelle teljingar i arkiva i Datatilsynet. Talet på omgjeringar og oversendingar til Personvernnemnda overstig talet på klager med éi sak. Årsaka kan vere at ei sak er omgjord utan formell klage.

skulle kome i konflikt med interessene til Justisdepartementet som etatsstyrar av fleire store behandlingsansvarlege.

Arbeidsfordelinga mellom departementa fungerer bra. Departementa har eit godt samarbeid om saker på personvernområdet der det er naturleg og nødvendig. Datatilsynet, som er knytt til begge departementa, meiner oppgåvefordelinga fungerer tilfredsstillande og ikkje er vanskeleg å innrette seg etter.

Det ligg ikkje føre konkrete planar om å endre den noverande arbeidsfordelinga på personvernområdet. Det sentrale er at dei departementa som har ansvar på personvernområdet, samarbeider om å gjennomføre dei ulike oppgåvene til det beste for personvernet. Det er òg viktig at andre departement med sektoransvar er medvitne om ansvaret dei har for å ta hand om personvern på kompetanseområdet sitt.

10.9 Samandrag og tilrådingar

Regjeringa ser det slik at personvernstyremakta i hovudsaka fungerer tilfredsstillande og gjer godt arbeid med etter måten små ressursar. Den raske teknologiske utviklinga inneber krevjande og stadig større oppgåver for Datatilsynet. Mange av oppgåvene kan best løysast ved internasjonalt samarbeid, og det er viktig at Datatilsynet deltek i internasjonalt personvernarbeid for å finne fram til felles løysingar på desse utfordringane. Slikt arbeid er ressurskrevjande. Regjeringa vurderer frå år til år om og eventuelt kor mykje budsjettet til Datatilsynet skal aukast for at dei skal kunne ta hand om oppgåvene sine på ein god måte.

Regjeringa ser det slik at personvernrådgivarar med klåre oppgåver og ei sterk forankring i leiinga i verksemda kan ha positiv effekt på korleis verksemder tek hand om personvernomsyn, og slik sett òg personvernet. Regjeringa vil derfor vurdere endringar i ordninga med personvernombod/personvernrådgivarar i lys av EUs revisjon av personverndirektivet.

Boks 10.1 Hovudpunkt kapittel 10

- 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.

11 Økonomiske og administrative konsekvensar

Personopplysningsregelverket skal gi rammer for rett bruk av personopplysningar for både dei registrerte og dei som skal behandle personopplysningar. Denne meldinga går gjennom og vurderer korleis handlingsrommet i personopplysningsregelverket kan nyttast til beste for både dei registrerte og dei behandlingsansvarlege. Det blir tilrådd ulike generelle løysingar og tiltak for så god ivaretaking av personvernet som råd. Eitt eksempel er ivaretaking av retten til anonymitet gjennom auka bruk av personvernfremjande teknologi, eit anna er ivaretaking av retten til informasjon gjennom elektroniske innsynsløysingar.

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 regelverket. 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. For eksempel kan system som opnar for trygg innlogging og elektronisk innsyn i personopplysningar minske behovet for manuell handtering av førespurnader frå dei registrerte. Det kan i sin tur gi reduserte administrative kostnader. 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.

Både for dei registrerte og for dei som skal behandle personopplysningar, kan det ta noko tid å tilpasse seg tilrådingane som er gitt, og konsekvensane av dei. Effekten av tiltaka kan derfor 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. Meldinga inneheld heller ikkje framlegg om konkrete tiltak eller konkrete regelendringar der kostnadene beint lèt seg rekne ut. Det er derfor ikkje råd å rekne konkret ut dei økonomiske eller administrative konsekvensane av dei generelle tilrådingane i 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.

Fornyings-, administrasjons- og kyrkjedepartementet

t i l r å r :

Tilråding frå Fornyings-, administrasjons- og kyrkjedepartementet 14. desember 2012 om Personvern – utsikter og utfordringar blir send Stortinget.

Offentlege institusjonar kan tinge fleire eksemplar frå:
Servicesenteret for departementa
Internett: www.publikasjoner.dep.no
E-post: publikasjonsbestilling@dss.dep.no
Telefon: 22 24 20 00

Opplysningar om abonnement, laussal og pris får ein hjå:
Fagbokforlaget
Postboks 6050, Postterminalen
5892 Bergen
E-post: offpub@fagbokforlaget.no
Telefon: 55 38 66 00
Faks: 55 38 66 01
www.fagbokforlaget.no/offpub

Publikasjonen er også tilgjengeleg på
www.regjeringa.no

Forsidebilete: Shutterstock/Semisatch

Trykk: 07 Oslo AS 12/2012