NOU Norges offentlige utredninger 2009: 1

Individ og integritet

Personvern i det digitale samfunnet

Norges offentlige utredninger
2009

Seriens redaksjon:
Departementenes servicesenter
Informasjonsforvaltning

---

1. Individ og integritet.
   Fornyings- og administrasjonsdepartementet.

NOU Norges offentlige utredninger 2009: 1

Individ og integritet

Personvern i det digitale samfunnet

Utredning fra Personvernkommisjonen oppnevnt ved kongelig resolusjon 25. mai 2007.
Avgitt til Fornyings- og administrasjonsdepartementet 13. januar 2009.

Departementenes servicesenter
Informasjonsforvaltning

Oslo 2009

ISSN 0333-2306
ISBN 978-82-583-0997-7

07 Gruppen AS, Oslo

Til Fornyings- og administrasjonsdepartementet

Kommisjonen som ble oppnevnt ved kongelig resolusjon 25. mai 2007 for å foreta en utredning om personvern, legger med dette fram sin utredning.

Oslo 13. januar 2009

Kjellbjørg Lunde
leder

Hans Antonsen	Gunnar Flikke	Ann Rudinow Sætnan
Gro Snortheimsmoen Bergfjord	Rune Fløisbonn	Michael Tetzschner
Lee A. Bygrave	Gisle Hannemyr	Sandra Qian Xiao
Inge Carlén	Mari Bø Haugstad	Henriette Sinding Aasen
Kjersti Fjørtoft	Grete Myhre	

Line Coll
Christine Lie Ulrichsen
Sekretariat

Innhold

Del I Innledning ... 9

1 Utredningsoppdraget og kommisjonens mandat ... 11
1.1 Personvernkommisjonens sammensetning ... 11
1.2 Personvernkommisjonens mandat ... 11
1.3 Personvernkommisjonens arbeid ... 13

2 Sammendrag av rapporten ... 17
2.1 Del I – Innledning ... 17
2.2 Del II – Personvernrett, hovedtrekk og hovedutfordringer ... 18
2.3 Del III – Det teknologiske landskapet ... 19
2.4 Del IV – Særskilte områder kommisjonen har arbeidet med ... 19
2.4.1 Personvern og media ... 19
2.4.2 Personvern for barn og unge ... 20
2.4.3 Personvern i arbeidslivet ... 21
2.4.4 Personvern i helsesektoren ... 22
2.4.5 Personvern i samferdselssektoren ... 24
2.5 Del V – Andre områder kommisjonen har arbeidet med ... 25
2.5.1 Organisering av personvernmyndighetene ... 25
2.5.2 Grunnlovsfesting av personvernet ... 26

3 Økonomiske og administrative konsekvenser ... 27
3.1 Tiltak som vil gi økt proveny ... 27
3.2 Tiltak som er betinget av midler til drift, prosjektarbeide eller utredning ... 27
3.3 Tiltak som krever kompetanseheving ... 28
3.4 Tiltak med administrative konsekvenser ... 28

4 Utgangspunkt og avgrensinger ... 29
4.1 Nærmere om begrepet personvern ... 29
4.1.1 Begrepets fødsel og opprinnelige betydning ... 29
4.1.2 Et særnorsk begrep ... 30
4.1.3 Personvernbegrepets røtter ... 30
4.1.4 Nyere litteratur og forsøk på avgrensing av begrepet ... 31
4.1.5 Skillet mellom «personvern» og «personopplysningsvern» ... 32
4.1.6 Begrepene personvern og rettssikkerhet ... 32
4.2 Det verdimessige grunnlaget for personvern ... 34
4.2.1 Personvern og personopplysninger ... 34
4.2.2 Glimt fra samfunnsforskning om personopplysningers relevans for håndtering av sosiale relasjoner ... 35
4.2.3 Personvern og personlig integritet ... 36
4.2.4 Vern av privatlivets fred ... 37
4.2.5 Rett til privatliv: Individuell frihet og kollektivt gode ... 38
4.3 Undersøkelser om personvernets stilling ... 40
4.4 Overvåkning og kontroll ... 41
4.4.1 Echelon, FRA-loven og EUs datalagringsdirektiv ... 42
4.4.2 Kommersielle selskapers overvåkning av sine brukere ... 44
4.4.3 Økonomisk regulering av personvernulemper ... 44
4.5 Fra data til personopplysninger ... 45
4.5.1 Data og informasjon ... 45
4.5.2 Opplysninger ... 45
4.5.3 Personopplysninger ... 45

Del II Personvernrett – hovedtrekk og hovedutfordringer ... 51

5 Innledning ... 53

6 Internasjonale regler ... 54
6.1 Personvern etter menneskerettighetstraktater ... 54
6.1.1 FN-konvensjonen om sivile og politiske rettigheter av 1966 ... 54
6.1.2 FN-konvensjonen om barns rettigheter av 1989 ... 55
6.1.3 Den europeiske menneskerettskonvensjon av 1950 ... 55
6.1.4 EUs charter om grunnleggende rettigheter av 2000 ... 56
6.2 Internasjonale regelsett som direkte angår personvern ... 56
6.2.1 Europarådets konvensjon av 1981 ... 56
6.2.2 OECDs retningslinjer av 1980 ... 57
6.2.3 FNs retningslinjer av 1990 ... 57
6.2.4 EUs direktiv 95/46 ... 57
6.2.5 Sektorvise direktiv ... 60
6.2.6 Norges spillerom ved utforming av personvernregelverk ... 60

7 Nasjonalt regelverk om personvern ... 61
7.1 Personopplysningsloven ... 61
7.1.1 Hovedtrekkene i personopplysningsloven ... 61
7.1.2 Datatilsynet og Personvernnemnda ... 62
7.2 Personvernbestemmelser i særlovgivningen ... 63
7.2.1 Folkeregisterloven ... 63
7.2.2 Helseregisterloven ... 63
7.2.3 Helseforskningsloven ... 64
7.2.4 Regelverk om politiets behandling av personopplysninger ... 64
7.2.5 Arbeidsmiljølovens regler om kontrolltiltak på arbeidsplassen ... 65
7.2.6 Vern mot offentlig meddelelse av personlige eller huslige forhold ... 66
7.2.7 Vern mot personfotografering og retten til eget bilde ... 66
7.2.8 Vern av omdømme ... 67
7.2.9 Vern av konfidensialitet ... 67
7.2.10 Sektorvise bestemmelser om anonymisering/sletting av personopplysninger ... 68
7.3 Ulovfestede regler ... 68
7.4 Revisjon og etterkontroll av regelverket ... 69
7.5 Grunnlovsfesting av personvernet ... 70
7.6 Er regelverket om personvern vanskelig tilgjengelig? ... 71
7.7 Ivaretakelse av personvernhensyn ved implementeringen av nye lover ... 72

Del III Det teknologiske landskapet ... 73

8 Innledning ... 75

9 Teknologiske trender som utfordrer personvernet ... 78
9.1 Nanoteknologi ... 78
9.2 Kommunikasjonsteknologi ... 78
9.3 Integrerte dataprosessorer i produkter ... 79
9.4 Radiofrekvensidentifikasjon ... 80
9.5 Elektroniske brikker og kort ... 81
9.6 Sensorteknologi ... 81
9.7 Biometri ... 82
9.8 Trådløs kommunikasjon og lokaliseringssporing ... 83
9.9 Internettavlytting ... 83
9.10 Digitalt fjernsyn ... 83
9.11 DNA-profilering ... 84
9.11.1 DNA-registeret i Norge ... 84

10 Personvernfremmende teknologier ... 86
10.1 Enkle personvernfremmende teknologier ... 86
10.1.1 Personlig datasikkerhet ... 86
10.1.2 Anonyme alternativer ... 86
10.1.3 Tilbaketrekking som gjør anonymitet mulig ... 87
10.1.4 Søkemotorimmunisering ... 87
10.1.5 Kryptering ... 87
10.2 Teknologier for identitetsforvaltning ... 88

11 Forslag til tiltak ... 89

Del IV Særskilte områder kommisjonen har sett på ... 91

12 Innledning ... 93

13 Personvern og media ... 94
13.1 Sentrale begreper ... 94
13.1.1 Forholdet mellom personvern og ytringsfrihet ... 94
13.1.2 Om begrepet massemedia ... 94
13.1.3 Om begrepene offentlighet og privatliv ... 95
13.2 Regulering ... 97
13.2.1 Lover, forskrifter og internasjonale konvensjoner ... 98
13.2.2 Rettspraksis ... 101
13.2.3 Forvaltningspraksis ... 106
13.2.4 Yrkesetiske retningslinjer ... 107
13.2.5 Avtaler ... 110
13.2.6 Allmennmoralen ... 111
13.3 Medietyper og medieroller ... 111
13.3.1 Redigerte media ... 111
13.3.2 Etter-redigerte media ... 111
13.3.3 Media som samler brukerinformasjon ... 112
13.3.4 Egenpubliserte media ... 114
13.3.5 «Media» i den private sfære ... 114
13.3.6 Medietyper: Oppsummering ... 115
13.3.7 Roller ... 115
13.3.8 Retten til anonymitet ... 116
13.4 Skattelister og pliktavlevering av elektronisk materiale ... 117
13.4.1 Offentliggjøring av skattelistene ... 117
13.4.2 Pliktavlevering av elektronisk materiale ... 118
13.5 Forslag til tiltak ... 120
13.5.1 Medieansvarslov ... 120
13.5.2 Fotografering, og retten til eget bilde ... 121

13.5.3 Utvidelse av fri rettshjelpordningen 122
13.5.4 Organ for nettytringer..... 122
13.5.5 Slettehjelp..... 125
13.5.6 Offentliggjøring av skattelistene..... 125
13.5.7 Pliktavlevering av elektronisk materiale..... 126
13.5.8 Internasjonalisering av nettregulering 126

14 Personvern for barn og unge 128
14.1 Sentrale problemstillinger 129
14.2 Det rettslige utgangspunktet 130
14.2.1 Menneskerettighetene..... 130
14.2.2 Personopplysningslovens samtykkebestemmelser..... 131
14.2.3 Barnelovens regler om foreldreansvaret og barnets beste 132
14.2.4 Ivaretakelse av personvernet i opplæringsloven og barnehageloven 133
14.3 Kommisjonens observasjoner 133
14.3.1 Innledning 133
14.3.2 Tilfredsstillende samarbeid mellom fagmyndigheter?..... 134
14.3.3 Holdninger og digital dømmekraft..... 134
14.3.4 Digital mobbing og personvernkrenkelser på nettet..... 136
14.3.5 Bruk og misbruk av opplysninger om egne barn 137
14.3.6 Markedsføring rettet mot barn 139
14.3.7 Personvern i skolesektoren..... 139
14.3.8 RFID-og GPS-sporing 145
14.3.9 Personvern for førskolebarn 145
14.4 Forslag til tiltak..... 145
14.4.1 Tiltak for å trygge barn og unges rettsikkerhet og personvern..... 145
14.4.2 Styrking av personvernet ved bruk av digitale media 146
14.4.3 Personvernansvarlig i skolen..... 146
14.4.4 Synlige etater på nettet 147
14.4.5 Opplysningsarbeid og annet holdningsskapende arbeid 147
14.4.6 Delta på arenaer der det er mulig å påvirke internasjonale regler..... 147

15 Personvern i arbeidslivet 149
15.1 Innledning og problemstilling..... 149
15.1.1 Utviklingstrekk 149
15.1.2 Personvernhensyn i norsk arbeidsliv 150
15.1.3 Aktuelle spørsmål..... 151
15.2 Rettslig regulering på området 151
15.3 Teknologiske utviklingstrekk som kan true personvernprinsippene.....154
15.4 Kommisjonens observasjoner og tilrådninger 155
15.4.1 Generelle betraktninger 155
15.4.2 Innsyn i e-post og elektroniske dokumenter.....156
15.4.3 Varslingsreglene 157
15.4.4 Rettslig plassering av reglene.....158
15.4.5 Andre tiltak som bør vurderes.....158

16 Personvern i helsesektoren 160
16.1 Utviklingstrekk.....161
16.2 Grunnleggende hensyn og spenningsforholdet mellom dem 162
16.3 Pasientjournalen og IKT-utviklingen.....163
16.4 Rettigheter, plikter og rettslig regulering 164
16.4.1 Retten til privatliv 164
16.4.2 Krav til behandling av personopplysninger og helseopplysninger.....165
16.4.3 Helsepersonells og andre yrkesgruppers taushetsplikt 166
16.5 Personvernkommisjonens observasjoner.....170
16.5.1 Elektronisk pasientjournal – EPJ.....170
16.5.2 Bør pasienten få tilgang til egne journalopplysninger i elektronisk format? 173
16.5.3 Personvern og praktisering av offentlighet.....174
16.5.4 Personvern og kontroll 175
16.5.5 Samarbeid og informasjons-utveksling. Særlig om NAV-reformen 175
16.5.6 Registre og de mange gode formål ...178
16.6 Kommisjonens anbefalinger og forslag til tiltak.....182
16.6.1 Kommunikasjon med pasienter 182
16.6.2 Utelatelse av individualiserende kjennetegn 182
16.6.3 System for identitetsadministrasjon..182
16.6.4 Personvernvennlig bruk av elektronisk pasientjournal (EPJ) 182
16.6.5 Gjennomgang av reglene for taushetsplikt.....183
16.6.6 Forbedring av pasienters rett til innsyn i journallogg 183
16.6.7 Opplærings- og holdningsskapende tiltak, innføring av bedre rutiner 183
16.6.8 Personvernfremmende tiltak ved opprettelsen av nye registre 183

16.6.9 Gjennomgang av dagens helseregistre ... 184

17 Personvern i transport og kommunikasjonssektoren ... 185
17.1 Hvordan utfordrer samferdsel personvernet? ... 185
17.2 Effektivitetsmessige krav ... 186
17.3 Trafikksikkerhetsmessige hensyn ... 187
17.4 Bekjempelse av kriminalitet og terror ... 188
17.4.1 Transportsektoren ... 188
17.4.2 Kommunikasjonssektoren ... 189
17.4.3 Rettslig regulering på området ... 191
17.4.4 Kommunikasjonsvern etter EMK ... 191
17.4.5 Vern mot overvåkning av offentlig ferdsel etter EMK ... 192
17.4.6 Kommunikasjonsvern etter norsk rett ... 193
17.4.7 Regler for bruk av kryptografi ... 194
17.4.8 Personopplysningsloven ... 194
17.5 Personvernkommisjonens observasjoner ... 196
17.6 Personvernkommisjonens tilrådninger ... 197

Del V Andre områder kommisjonen har arbeidet med ... 199

18 Organisering av personvernmyndighetene ... 201
18.1 Innledning ... 201
18.1.1 Rettslig forankring ... 201
18.1.2 Ledelse, arbeidsoppgaver, budsjett og årsverk ... 202
18.2 Personvernkommisjonens observasjoner ... 203
18.2.1 Om begrepene «ombud» og «tilsyn» ... 203
18.2.2 Om vedtak i Datatilsynet og Personvernnemnda ... 205
18.2.3 Om Personvernnemnda ... 206
18.2.4 Om direktørens tilsettingsform ... 206
18.2.5 Om tilsynets profesjonssammensetning ... 206
18.2.6 Om personvernombudene ... 206
18.3 Forslag til tiltak ... 207
18.3.1 Oppgaver ... 207
18.3.2 Økte ressurser til Datatilsynet ... 207
18.3.3 Regionalisering av Datatilsynet ... 207
18.3.4 Et råd for Datatilsynet ... 208
18.3.5 Sektorvis styrking av personvernkompetansen ... 208
18.3.6 Samarbeide med eksterne aktører ... 208
18.3.7 Dialog med akademia og andre fagmiljøer ... 208

19 Grunnlovsfesting av personvernet ... 209
19.1 Bakgrunn ... 209
19.2 Kort om utredningen ... 209
19.3 Personvernkommisjonens vurdering ... 209
19.4 Konklusjon ... 210

Direktiver omtalt i rapporten ... 211

Lover og forskrifter omtalt i rapporten ... 212

Litteraturliste ... 214

Vedlegg
1 Uttalelse om datalagringsdirektivet ... 221
2 Nemnd for Internett ... 224
3 Betenkning om grunnlovsfesting av retten til personvern/privatliv ... 244
4 Personvernøkende teknologi og identitetsforvaltning ... 276

Del I
Innledning

Kapittel 1
Utredningsoppdraget og kommisjonens mandat

1.1 Personvernkommisjonens sammensetning

Personvernkommisjonen ble nedsatt av Regjeringen den 25. mai 2007. Kommisjonen ble gitt følgende sammensetning:

Leder: Kjellbjørg Lunde, utdanningsdirektør hos fylkesmannen i Hordaland

- Hans Antonsen, ordfører Grimstad kommune
- Gro Snortheimsmoen Bergfjord, pasientombud i Rogaland
- Lee A. Bygrave, førsteamanuensis dr. juris UiO
- Inge Carlén, styremedlem i Landsrådet for Norges barne- og ungdomsorganisasjoner og student
- Kjersti Fjørtoft, post doc, dr. art UiT
- Gunnar Flikke, tidligere sjefredaktør i Adresseavisen
- Rune Fløisbonn, avdelingsdirektør Kripos
- Gisle Hannemyr, universitetslektor UiO
- Mari Bø Haugstad, dommer i Sør Østerdal tingrett
- Grete Myhre, direktør for Statens havarikommisjon for transport
- Ann Rudinow Sætnan, professor dr. polit NTNU
- Michael Tetzschner, advokat, advokatfirmaet Tetzschner og co
- Sandra Qian Xiao, avdelingsdirektør Telenor Broadcast
- Henriette Sinding Aasen, professor dr. juris UiB

Cand. jur. Line Coll var sekretær for kommisjonen fra 1. juni 2007 til og med 27. juni 2008, mens cand. jur. Christine Lie Ulrichsen, tiltrådte som sekretær 9. juni 2008 og hadde stillingen ut perioden. Gisle Hannemyr har i tillegg til å være medlem, også vært ansatt i sekretariatet. Kommisjonens sekretariat har vært ledet av Lee Bygrave.

1.2 Personvernkommisjonens mandat

Kommisjonens mandat lyder:

1. *Innleiing*
   Personvern kan verte definert på ulike vis. Sentralt i omgrepet står at kvart einskilt menneske er ukrenkjeleg og har krav på respekt frå andre menneske, for eigen integritet og for fred i sitt privatliv. Personvern er såleis nært knytt til einskildindividet sitt høve til privatliv, sjølvråderett (autonomi) og sjølvutfalding. Retten til privatliv følgjer mellom anna av den europeiske menneskerettskonvensjonen (EMK) artikkel 8, og står sentralt i EU sitt personverndirektiv (95/46 EF). Som andre grunnleggjande rettar må retten til privatliv og vernet til den einskilde sin integritet vegast opp mot andre sentrale rettar og verdiar. Retten til å hegne om personopplysningar kan til dømes komme i konflikt med retten til frie ytringar eller med samfunnet sin trong for vern mot kriminelle handlingar.
2. *Utfordringar for personvernet*
   Eit trekk ved samfunnsutviklinga er ei stadig aukande registrering og bruk av personopplysningar innafor alle sektorar, offentleg/privat og nasjonalt/internasjonalt. Den tekniske, administrative og økonomiske utviklinga fører i seg sjølv til auka innsamling, lagring og samankopling av informasjon. Stadig fleire daglege handlingar etterlet seg registrerte og logga elektroniske spor. Dette reiser mellom anna spørsmål om korleis ein skal sikre at det i visse samanhangar framleis skal vere mogleg for den einskilde å opptre anonymt. Det er òg ei utvikling i retning av meir utveksling av personopplysningar på tvers av landegrenser. Det har ført til ei rad med samarbeidsavtalar mellom land om utveksling av personopplysningar. Opplysningar som vert publiserte på Internett i eit land vert samstundes publiserte internasjonalt.

   I St.meld. nr. 17 har regjeringa peikt på den sårbare stillinga personvernet har i møte med

den teknologiske utviklinga, der mange kryssande omsyn og verdiar gjer seg gjeldande. Personvernet er sårbart mellom anna fordi det lett kan verte bytta bort i økonomiske eller praktiske føremoner for den som til dømes ønskjer å ta i bruk ei ny teneste, tilsynelatande utan ei grundig vurdering av at det aukar registreringa av personopplysningar og av kva for utfordringar dette kan ha for personvernet.

Ny teknologi har vorte tilgjengeleg for privatpersonar som òg kan nytte desse til å overvake andre. Folk sin tilgang til Internett, mobiltelefoni med kamera mv. fører til at personvernet også vert utfordra av naboar og vener. Meir bruk av ny teknologi kan såleis utfordre personvernet. På den andre sida kan ny teknologi vere med på å styrkje personvernet, mellom anna ved å gjere det enklare for den einskilde å få innsyn i kva for opplysningar som finst om ein, og til å gjere samfunnet meir ope. Teknologien kan òg på andre vis innrettast og brukast slik at han styrker personvernet. Ut frå eigne erfaringar, kunnskapar og opplevingar, vil kvar og ein ha ulik oppfatning av kor viktig det er å ta vare på personvernet i einskilde saker. Undersøkingar syner at folk gjennomgåande ser på personvern som eit viktig gode, men at dei til dels har dårlege formelle kunnskapar om reglar som varetek personvernet. Det same gjeld verksemder: Forholdet mellom krav i lov og formell etterleving er ikkje heilt som lova føreset, sjølv om verksemdene meiner det er viktig å ta vare på personvernet. Internasjonalt bindande reglar og europeisk og norsk personvernlovgiving har særleg merksemd på den einskilde sin sjølvråderett over eigne personopplysningar. I kva grad det er samfunnet eller det einskilde individet som skal ta avgjerda om korleis personopplysningar skal nyttast, er eit viktig prinsipielt spørsmål. Eit anna sentralt spørsmål er korleis samfunnet kan legge til rette for at den einskilde betre kan hegne om sitt eige personvern. Mange utfordringar for personvernet er sektorovergripande, andre gjeld særskilt for enkelte sektorar. Helsesektoren er eit av fleire område der personvernutfordringane er mange og vanskelege. Opplysningar om helse og sosiale omstende er rekna mellom dei mest private og sensitive opplysningane i samfunnet vårt. Samstundes er det i pasienten si interesse at legar og helseinstitusjonar har tilstrekkeleg informasjon. Helseforsking er eit anna tema som syner dilemma mellom trongen til å skjerme individet og samstundes kunne utvikle betre kunnskap og nye behandlingar. Innafor samferdselssektoren er det personvernutfordringar knytte til m.a. lagring av trafikkinformasjon (tele, Internett mv.), system for betaling som krev registrering av rørsler (elektroniske system for betaling i vegtransport, elektronisk billettering i kollektivtrafikk) tryggleik, (automatisk trafikk-kontroll, kameraovervaking i kollektive transportmedel) og ny kjøretøyteknologi (system som syner posisjonering, «e-safety» mv.). I arbeidslivet generelt er det ein diskusjon for og mot aukande kontrollverksemd overfor eigne tilsette gjennom til dømes e-post/mobil og kameraovervaking, biometri og GPS. Barn og unge er ivrige i bruken av nye elektroniske kommunikasjonsformar, t.d. SMS/MMS «chatting», «YouTube». Unge er difor oftast i forkant i utviklinga av nye tenester og nye måtar å nytte teknologi på. Ein bør difor óg ha særkild merksemd mot denne gruppa. Media vil i mange høve søke å setje saman og presentere personopplysningar som dei sankar inn frå ulike kjelder. Sjølv om ein held utafor det som skjer ved hjelp av ulovlege metodar, syner dette at det er viktig å vurdere kor sterkt personvernet bør stå seg mot medias adgang til lovlege opplysingar om den einskilte. Løysingane på personvernutfordringane må òg balanserast mot andre omsyn, som omsynet til innovasjon og utvikling i næringslivet.

3. *Oppdraget*

   Kommisjonen skal på denne bakgrunn:
   - Gi ein heilskapleg 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.
   - Vurdere nærare korleis personvernet bør takast vare på i møtet 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 òg 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.

Regjeringa ønskjer ei heilskapleg vurdering av korleis personvernet til den einskilde kan verte teke vare på som ein del av den vidare samfunnsutviklinga. Regjeringa meiner òg det er naudsynt å vurdere og å leggje til rette for utvikling av personvernfremjande teknologi. Slik teknologi vil kunne sikre at personvernet blir ein integrert del av nye løysingar, samstundes som slik teknologi kan gjere det enklare for folk å ta vare på rettane sine. Regjeringa ønskjer eit auka engasjement, ein brei debatt og ei utgreiing av utfordringane vi står framfor med omsyn til personvernet. Kommisjonen skal difor innrette verksemda si slik at den stimulerer til debatt ved å setje personvernspørsmål på dagsordenen, og på den måten bidra til auka merksemd om personvern generelt i befolkninga. Kommisjonen står fritt til å ta opp alle omstende han meiner er relevante for vurderinga av personvernet. Kommisjonen skal likevel ikkje fremje konkrete lovforslag eller ta stilling til konkrete spørsmål om lovgiving som fell inn under det pågåande arbeidet med etterkontroll av personopplysningslova i regi av Justisdepartementet. Kommisjonen kan levere ei eller fleire (del)utgreiingar. Kommisjonen må gjere greie for konsekvensane av dei forslaga som vert fremja, irekna dei økonomiske og administrative konsekvensane.

Kommisjonen skal rapportere til Fornyings- og administrasjonsdepartementet innan 15. desember 2008.

4. *Organisering*
Til rådvelde for kommisjonen vert det oppretta eit sjølvstendig sekretariat, uavhengig av departementet, med ein leiar og 2 sakshandsamarar knytt til universitetet i Oslo med ekspertar på personvernjuss og teknologi. Utgiftene skal dekkast over FAD sitt budsjett.

1.3 Personvernkommisjonens arbeid

Første regulære møte i Personvernkommisjonen ble avholdt 26. juni 2007. Kommisjonen har totalt hatt 39 møtedager. I tillegg var kommisjonen våren 2008 inndelt i fem arbeidsgrupper som har avholdt egne møter. Sekretariatet og leder har også møttes ved behov.

Fornyings- og administrasjonsdepartementet hadde forut for kommisjonens oppstart sendt ut et generelt brev til samtlige departementer og bedt om innspill til kommisjonens arbeid. I tillegg har Personvernkommisjonen bedt om innspill fra LO, NHO, Kystdirektoratet og Fiskeridirektoratet.

Kommisjonens nettsted (med adresse *www.personvernkommisjonen.no*) har vært i drift i hele kommisjonens funksjonstid og inneholder blant annet en presentasjon av Personvernkommisjonens medlemmer, en side for publikumskontakt, et løpende oppdatert arkiv over aktuelle personvernnyheter, en oversikt over aktuell personvernlitteratur, samt en side der dokumenter som kommisjonen har publisert (kronikker, delrapport om medier og personvern, uttalelse om datalagringsdirektivet) har blitt gjort tilgjengelig for publikum. I samband med at kommisjonen våren 2008 avholdt en serie åpne møter, ble det utviklet et nettbasert system der publikum kunne melde seg på disse. Presentasjoner fra møtene ble publisert på kommisjonens hjemmeside.

Personvernkommisjonens medlemmer har også hatt tilgang til et intranett. Dette ble benyttet for distribusjon av møtereferater og arbeidsnotater blant kommisjonens medlemmer.

Personvernkommisjonen har mottatt ca. ti henvendelser fra publikum, som har blitt besvart fortløpende. Innspillene fra publikum har sammen med de overnevnte innspill fra departementer, inviterte frivillige organisasjoner og direktorater, blitt brukt i kommisjonens arbeid.

De første månedene av kommisjonens arbeidsperiode ble brukt til intern opplæring og innføring i personvernrett og teknologi. Kommisjonens omfattende mandat og brede sammensetning gjorde det nødvendig å etablere en felles faglig plattform.

Basert på mandatets hovedfokus på samfunns- og problemområder, ble kommisjonen inndelt i følgende arbeidsgrupper fra første halvdel av 2008:

– Arbeidsgruppe for medier og personvern.
– Arbeidsgruppe for barn og unges personvern.
– Arbeidsgruppe for personvern i arbeidslivet.
– Arbeidsgruppe for personvern i helsesektoren.
– Arbeidsgruppe for personvern i samferdselssektoren.

Våren 2008 avholdt kommisjonen åpne debattmøter innenfor disse fagområdene. De åpne møtene har hatt flere funksjoner. For det første har møtene bidratt til å øke kommisjonens kunnskap og forståelse av ulike problemstillinger på personver-

nets område. For det andre har åpenheten gjort det mulig for interesserte å ta del i kommisjonens arbeid og komme med innspill. For det tredje har møtene skapt en viss løpende offentlig debatt om ulike problemstillinger knyttet til personvern og personopplysningsvern i dagens samfunn, i tråd med kommisjonens mandat. I forkant av de åpne møtene ble det sendt ut invitasjoner til antatt interesserte enkeltpersoner og organisasjoner, samt media. Samtlige møter ble avholdt i Oslo. Det var bra oppslutning på møtene og ulike fagmiljøer var godt representert.

Det første åpne møtet ble arrangert 7. februar 2008 og hadde tema «Media og personvern». Innlegg ble holdt av Georg Apenes (direktør i Datatilsynet), Rune Opdahl (advokat i Wiersholm, Mellbye & Bech), Ørnulf Røhnebæk (lagdommer og tidligere sekretær i Ytringsfrihetskommisjonen), Per Edgar Kokkvold (generalsekretær i Norsk Presseforbund), Kyrre Eggen (advokat i Wiersholm, Mellbye & Bech), Ina Lindahl (advokatfullmektig i Advokatfirmaet Hjort), Nils E. Øy (generalsekretær i Norsk Redaktørforening), Hilde Haugsgjerd (redaktør i Aften), Jan Omdahl (mediekommentator i Dagbladet), Knut Olav Åmås (debattredaktør i Aftenposten) og Hilde Sandvik (debattredaktør i Bergens Tidende).

Neste åpne møte hadde tema «Personvern for barn og unge» og ble avholdt 6. mars 2008. Seminaret ble åpnet av fornyings- og administrasjonsminister Heidi Grande Røys. Innledere var Elizabeth Hartmann (kommunikasjonsrådgiver og daglig leder Siste skrik reklamebyrå), Stian Lindbøl (seniorrådgiver Medietilsynet), Christine Hafskjold (prosjektleder Teknologirådet), Knut Haanes (nestleder Barneombudet), Thomas Hepsøe (prosjektleder Medietilsynet), Knut B. Kaspersen (avdelingsdirektør Datatilsynet) og Torbjørn D. Moe (Utdanningsdirektoratet). I tillegg var det et panel bestående av Martin Vonstad Østerdal, Mikal Kvamsdal og Yonas Bennour, alle elever på videregående skole.

Den 10. april 2008 arrangerte kommisjonen et åpent møte om «Personvern i arbeidslivet». Innlegg ble holdt av Astrid Flesland (seniorrådgiver Datatilsynet), Cecilie Wille Søvik (advokatfullmektig i Ræder advokatfirma), Nina Melsom (advokat i NHO), Sigurd-Øyvind Kambestad (advokat i LO), Claude A. Lenth (advokat i Hjort advokatfirma), Marit B. Frogner (advokat i Wiersholm, Mellbye & Bech), Mette Borchgrevink (advokat i Steenstrup Stordrange).

Neste møte ble avholdt 19. mai 2008, med temaet «Personvern i helsesektoren». Innlegg ble holdt av Ola Bergslien (sjefslege St. Olavs Hospital), Målfrid Frahm Jensen (pasient og erfaringskonsulent), Tor Johan Saglie (direktør Arbeids- og velferdsetaten), Sverre Engelschiøn (seniorrådgiver Datatilsynet), Ann Kristin Krokan (kommunikasjonskonsulent ULOBA), Hilde Jordal (prosjektleder Helsedirektoratet), Leif T. Aanesen (avdelingsdirektør Datatilsynet), Øystein Nytrø (førsteamanuensis NTNU), Heidi Thorstensen (personvernombud og IKT-sikkerhetssjef Ullevål Universitetssykehus).

Det siste åpne møtet ble avholdt den 10. juni 2008, og tittel for seminaret var «Personvern og samferdsel – reisen til Panoptikonet?». Innlegg ble holdt av Eva Hildrum (departementsråd i Samferdselsdepartementet), Dag Wiese Schartum (professor UiO), Tarald Johansen (seksjonsleder Security og beredskap Avinor), Kåre Halvorsen (sjefingeniør Statens havarikommisjon for transport), Torkel Bjørnskau (forskningsleder Transportøkonomisk institutt), Jens C. Koch (underdirektør Post og teletilsynet), Leif T. Aanensen (avdelingsdirektør Datatilsynet) og Ingvild Hanssen-Bauer (advokat ved advokatfirma Wikborg Rein).

Kommisjonen har også invitert eksterne foredragsholdere til sine interne møter, og har fått innspill fra Datatilsynets direktør Georg Apenes, leder for Personvernnemnda Jon Bing, professor Charles Raab ved Universitet i Edinburgh, professor Lucy Smith ved UiO, professor Erik Boe ved UiO, professor Thomas Mathiesen ved UiO, professor Dag Wiese Schartum ved UiO, forsker Tommy Tranvik ved UiO, stipendiat Thomas Olsen ved UiO, stipendiat Inger Marie Sunde ved UiO, Tore Tennøe og Christine Hafskjold fra Teknologirådet, advokat Kyrre Eggen, førsteamanuensis Svein Brurås fra journalistutdanninga i Volda, journalist og advokat Ane Sofie Tømmerås, politiadvokat Eirik Trønnes Hansen fra Kripos, professor Finn Arnesen ved UiO, personvernombud og IKT-sikkerhetssjef Heidi Thorstensen fra Ullevål universitetssykehus, Geir Kjønigsen fra Statens vegvesen, advokat Andreas Galtung og journalist Carl-Erik Grimstad.

Høsten 2008 jobbet kommisjonen videre med innspillene fra de åpne møtene, og gruppene og sekretariatet startet prosessen med å utarbeide konkret tekst til rapportens ulike kapitler.

Kommisjonen har også vært aktivt til stede i samfunnsdebatten med blant annet følgende kronikker forfattet av medlemmer av kommisjonen (Coll og Lunde 2008, Fløisbonn 2008, Hannemyr 2008b, Hannemyr 2008c, Hannemyr 2008a). Kom-

misjonen kom i juni 2008 med en uttalelse om Datalagringsdirektivet som ble referert og kommentert i et stort antall media. Mediearkivet, som er en database over Norges viktigste media på papir og på nett, oppgir at Personvernkommisjonen er omtalt i mediene 177 ganger i 2007 og 270 ganger i 2008 (til sammen 447 ganger). Av disse stammer 78 oppslag fra papiraviser og 369 fra ulike nettpublikasjoner. Personvernkommisjonens eget mediearkiv (som bare registrerer oppslag med substansielt innhold) har i kommisjonens funksjonstid fram til medio november registrert 144 medieoppslag som direkte handler om eller som kommenterer kommisjonens arbeid. Søkemotoren Sesam, som også tar for seg personlige hjemmesider og blogger har i samme periode indeksert om lag 4860 dokumenter på Internett som på et eller annet vis omtaler Personvernkommisjonen.

Når det gjelder opptredener på radio og tv, har Kommisjonens leder vært intervjuet en rekke ganger og uttalt seg både i forbindelse med personvernspørsmål generelt og om mer dagsaktuelle personvernsaker. Gunnar Flikke i Kurer (P2) i august 2008 og oktober 2008. Gisle Hannemyr i Kulturnytt (P2) i juni 2008, i Kurer (P2) i september 2008, i Norgesglasset (P1) i september 2008, og i Sånn er livet (P1) i desember 2008. Kjellbjørg Lunde i Kulturnytt (P2) i november 2008 og i Verdibørsen (P2)

Kommisjonens leder, kommisjonsmedlemmer og kommisjonens sekretariat har holdt foredrag og deltatt på en rekke møter og seminarer om personvern.

Kjellbjørg Lunde holdt innlegg på den årlige Personvernkonferansen i 2007 med temaet «Personvern – også i fremtiden?»

Rune Fløisbonn holdt innlegg på Teknologirådets frokostseminar om personvern i desember 2007.

Lee A. Bygrave arrangerte et internasjonalt symposium 22.-23. november 2007 i Oslo om «Body Control: Legal Regulatory Perspectives on Biometrics and Biobanks», der flere av kommisjonens medlemmer deltok. Bygrave selv holdt et innlegg med tittelen «Data Privacy Law and the Human Body – Oil and Water?». Bygrave har også holdt innlegg på flere andre internasjonale konferanser, herunder om «Consent versus Proportionality Principle: Are the Proportions Right?» på en konferanse den 12. oktober 2007 i Brussel med tittel «Reinventing Data Protection?»; et innlegg om «The Data Retention Directive in the Norwegian Legal Context» på en konferanse den 14. mai 2008 ved Universitetet i Bergen med tittel «The Data Retention Directive: Will it make a Difference?»; og et innlegg om «How to Build Privacy Protection: A Present Day View of Choices and Difficulties» på en konferanse den 19. november 2008 ved Stockholms Universitet med tittel «IT Regulations and Policies – From Theory into Practice». Bygrave holdt også innlegg den 5. mars 2008 for UK House of Lords Constitution Committee i Westminster, London i forbindelse med komiteens utredning om «The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their relationship with the State». Bygrave deltok videre på et «nettforum» i regi av Aftenposten den 25. januar 2008 der han svarte på spørsmål fra publikum om EUs datalagringsdirektiv og personvern på Internett.

Henriette Sinding Aasen holdt innlegg på ovennevnte symposium (*Body Control – Legal Regulatory Perspectives on Biometrics and Biobanks*) med tittelen «Biobank Law in Norway – Critical Reflections». Videre holdt hun et innlegg på Pediaterdagene i oktober 2008 med temaet «Legens plikter og rettigheter i forhold til media og pårørende».

Gisle Hannemyr presenterte Personvernkommisjonens arbeide i eNorge-forum i juni 2008 og holdt innlegg og deltok i paneldebatt om media og personvern på Norsk redaktørforenings årsmøte i oktober 2008, holdt innlegg på SINTEFs konferanse i juni 2008 om «Personvern i rike medier» og deltok på nettdebatt arrangert av Aftenposten som den svenske FRA-loven i oktober 2008. Han har også holdt innlegg om media og personvern i interdepartemental referansegruppe i desember 2008.

Inge Carlén holdt innlegg på Personvernkonferansen i desember 2008 hvor temaet var personvern i skolen.

Michael Tetzschner deltok på FAFOs frokostmøte om personvern i arbeidslivet i november 2008 og holdt foredrag for journaliststudentene for Norges kreative fagskole i desember 2008.

Kjersti Fjørtoft holdt innlegg om «Personvern i skolen» på skolelederkonferansen i november 2008 hvor temaet var Skolen i digital utvikling, og om personvern generelt på Lørdagsuniversitetet i regi av Universitetet i Tromsø.

Ann Rudinow Sætnan deltok på BioCentre symposium: «Privacy and Surveillance: Monitoring Humans and Monitoring Human Rights», arrangert av House of Lords i London i mai 2008. Hun deltok videre på arrangementene Society for Social Studies of Science & European Association

for the Study of Science and Technology i Rotterdam, august 2008 og Medical Sociology Study Group Annual Meeting, i regi av British Sociological Association, University of Sussex, Brighton. På begge disse samlingene presenterte hun følgende paper: «Numbers as Privacy? Statistics as interface between the personal and the political». Sætnan bidro også på en workshop organisert av ESRC Genomics Forum, University of Edinburgh, i oktober 2008 hvor temaet var «Genetic Suspects: Emerging Forensic Uses of Genomic Technologies». Her holdt hun foredrag med tittelen: «DNA databases, datasharing and function creep».

Gisle Hannemyr og Mari Bø Haugstad deltok på den store personvernkonferansen i Montreal i september 2007.

Gunnar Flikke holdt foredrag i Norsk Presseforbunds hovedstyre i november 2008 og for Landsstyret i Norsk Journalistlag i desember 2008 om temaet media og personvern.

Kommisjonen har vært på to studieturer til henholdsvis Stockholm og London. Målet har vært å skaffe seg kunnskap om det tilsvarende arbeidet som er utført i disse to landene. I Stockholm ble det avholdt møte med den svenske Integritetsskyddskomiteen, den svenske Datainspeksjonen og med professor Peter Seipel og professor Cecilia Magnusson Sjöberg ved Universitetet i Stockholm.

I London ble det avholdt møter med Dr. Gus Hosein, London School of Economics (LSE), House of Lords Constitution Committee og House of Commons Home Affairs Committee.

Av tidsmessige årsaker var det nødvendig for kommisjonen å engasjere ekstern utredningshjelp i forhold til noen sentrale områder. Advokat Andreas Galtung har skrevet en utredning om nemnd for Internett, se vedlegg 2 til rapporten. Stipendiat Thomas Olsen, ved Institutt for privatrett, Universitetet i Oslo, har skrevet om personvernfremmende teknologier og identitetsforvaltning. Arbeidet er inntatt som vedlegg 4 til rapporten. Professor Alf Petter Høgberg og forsker Njål Høstmælingen har gitt en betenkning om grunnlovsfesting av personvernet. Arbeidet er inntatt som vedlegg 3 til rapporten.

Flere av kommisjonens medlemmer har levert skriftlige bidrag i løpet av prosessen. Noen av disse bidragene er tatt direkte inn som underkapitler. Utredningen er ellers ført i pennen av kommisjonens sekretariat. Flere bidragsytere kan forklare eventuelle ulikheter i uttrykksform og språkbruk.

Kapittel 2
Sammendrag av rapporten

Fra regjeringen fikk Personvernkommisjonen i oppdrag å gi en helhetlig vurdering av hvordan personvernet til den enkelte kan ivaretas i en tid hvor samfunnsutviklingen medfører en stadig økende registrering og bruk av personopplysninger. Personvernet er under press, både som følge av den teknologiske, administrative og økonomiske utviklingen.

Kommisjonen ble blant annet bedt om å gi en oversikt over hvilke utfordringer personvernet står overfor i dagens samfunn og samtidig vurdere hvordan personvernet bør ivaretas i møte med andre og ofte motstridende hensyn og verdier. Kommisjonen ble også bedt om å kartlegge og evaluere eksisterende virkemidler for ivaretakelse av personvernet og eventuelt fremme forslag til nye prinsipper og virkemidler.

For en nærmere oversikt over kommisjonens mandat og arbeid vises det til kapittel 1.2 og 1.3.

I dette kapittelet vil Personvernkommisjonen gi en oppsummering av rapportens innhold og forslag til tiltak. Rapporten består av fem hoveddeler, som igjen består av flere kapitler. Sammendrag av disse vil bli presentert kronologisk nedenfor.

Av tidsmessige årsaker har Personvernkommisjonen engasjert ekstern utredningshjelp i forhold til sentral områder hvor det var nødvendig med særlig ekspertise. Utredninger om nemnd for Internett, personvernfremmende teknologier og identitetsforvaltning og grunnlovsfesting av personvernet ligger som vedlegg til rapporten. Som vedlegg ligger også Personvernkommisjonens særlige uttalelse om Datalagringsdirektivet.

2.1 Del I – Innledning

I *kapittel 1* gis det en oversikt over utredningsoppdraget, kommisjonen mandat, kommisjonens sammensetning og kommisjonens arbeid. I mandatet presiserte regjeringen at den ønsket bred debatt om personvernet og kommisjonen ble derfor bedt om å innrette sin virksomhet slik at den bidro til å sette personvernspørsmål på dagsordenen. Kapittel 1 inneholder en oversikt over de eksterne møtene kommisjonen har avholdt for dette formålet, samt hvem som ellers har gitt innspill og i så måte vært sentrale premissleverandører for kommisjonens videre arbeid.

Kapittel 2 er dette sammendraget.

I *kapittel 4* gjøres det rede for kommisjonens utgangspunkt, samt en del avgrensninger det har vært nødvendig å gjøre.

«Personvern» er et begrep som har vært og vil være gjenstand for omfattende diskusjon, både i teori og praksis. Det har derfor vært viktig for kommisjonen å foreta en nærmere avgrensning av begrepets innhold. I *kapittel 4.1* skisserer Personvernkommisjonen både begrepets opprinnelige betydning og nyere forsøk på å avgrense og definere dette.

I Norge ble personvern tidlig knyttet til mer enn vern av privatlivets fred og den personlige integritet. Også ønsket om å ha kontroll over den informasjonen som beskriver en som individ sto i fokus. Det ble oppstilt ulike interesser som man mente at personvernet søkte å ivareta: blant annet diskresjon, innsyn, begrenset overvåkning og kontroll samt interesse i privatlivets fred. Disse interessene er fremdeles en vesentlig del av personvernbegrepet, men som en konsekvens av moderne informasjonsteknologi og nye metoder for innsamling og bruk av personopplysninger, har innholdet i definisjonen og kategoriseringen av vernede interesser blitt presisert og videreutviklet.

Etter Personvernkommisjonens oppfatning er det grunn til å foreta et skille mellom personvern og personopplysningsvern, både av pedagogiske hensyn og fordi man ser en utvikling i denne retningen i internasjonal personvernrett. Med *personvern* forstår kommisjonen ivaretakelse av personlig integritet, ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse. *Personopplysningsvern* mener kommisjonen dreier seg om regler og standarder for behandling av personopplysninger som har ivaretakelse av personvern som hovedmål.

Personvern har ikke bare en side mot juss og teknologi. For å danne seg et helhetlig bilde av personvernet har det derfor vært viktig for kommisjonen å gå nærmere inn på det verdimessige grunnlaget for personvern. I *kapittel 4.2* diskuteres derfor personvernet fra et filosofisk og samfunnsvitenskaplig perspektiv. Personvernet drøftes med utgangspunkt i hensynet til den enkeltes integritet og autonomi, hensynet til privatlivets fred, og hensynet til samfunnsdeltakelse og demokrati. Personvernet betraktes også i forhold til samfunnets interesser og andre rettigheter. Det konkluderes med at personvernet primært ikke må betraktes som et instrument for ytringsfrihet og fri offentlig diskusjon, men bør gis en selvstendig begrunnelse i menneskerettslige prinsipper og moralsk respekt.

I *kapittel 4.3* refereres tre nyere undersøkelser om personvernets stilling. Den første undersøkelsen viser at det er gjennomgående stor tillit i befolkningen til at personvernet blir tatt vare på. Den andre undersøkelsen viser at det blant virksomhetene er en grunnleggende positiv holdning til personvern, men at kunnskapen om personopplysningsloven og de kravene den stiller er lav. Den siste undersøkelsen er rettet mot transportsektoren og terrorbekjempelse, og viser at aktørene i denne sektoren har vurdert personvernimplikasjonene av sikkerhetstiltak i egen virksomhet, og at de oppfatter disse som uproblematiske.

I *kapittel 4.4* stilles personvernet opp mot overvåkning og kontroll, og særlig den omstendigheten at de teknologiske mulighetene som ligger i moderne systemer for overvåkning i enkelte tilfelle gjør overvåkningen så omfattende at den har totalitær karakter.

I den forbindelse foreslår Personvernkommisjonen følgende:

1. *Økonomisk regulering av personvernulemper.*
   Man kan i visse tilfeller regulere personvernulemper ved hjelp av økonomiske virkemidler ved å sette en kostnad (for eksempel i form av avgift) på tiltak som kan ha negativ effekt på personvernet. Som et eksempel på et område hvor slik avgiftsregulering kan være særlig aktuelt, nevner Personvernkommisjonen kameraovervåkning av det offentlige rom.

I *kapittel 4.5* defineres sentrale begreper som «data», «informasjon», «opplysninger» og «personopplysninger».

2.2 Del II – Personvernrett, hovedtrekk og hovedutfordringer

Gjennom mandatet ble kommisjonen oppfordret til å skildre dagens situasjon og utfordringer for personvernet innen ulike sektorer og se hen til internasjonale avtaler og regelverk om personvern.

Personvernretten er preget av omfattende regulering, både nasjonalt og internasjonalt. I *kapittel 6* gis det en oversikt over internasjonale instrumenter om personvern. Mange av disse nedfeller et stort antall minstekrav som Norge er forpliktet til å overholde ved utarbeidelsen av nasjonal personvernrett. Andre er av mer veiledende karakter. I dette kapittelet gjennomgås personvernbestemmelser etter menneskerettighetstraktater, relevante direktiver fra EU, samt andre retningslinjer og konvensjoner. I tillegg berøres noe sentral praksis fra EF-domstolen. Internasjonal personvernrett er også gjenstand for behandling og diskusjon i de delene av rapporten som omhandler mer spesifikke områder kommisjonen har arbeidet med.

I *kapittel 7* gir Personvernkommisjonen en oversikt over det nasjonale regelverket om personvern, uten at fremstillingen på noen måte kan sies å være uttømmende. Fokuset er rettet mot lovgivning som har hatt særlig relevans for kommisjonens arbeid. I tillegg blir personvernbestemmelser og sentrale juridiske problemstillinger innenfor de særskilte områdene kommisjonen har arbeidet med gjennomgått i rapportens *del IV*.

I norsk rett finnes det generelle personvernbestemmelser som gjelder innenfor alle bransjer og sektorer. Personopplysningsloven med forskrifter er særlig sentral her. I tillegg finnes det sektorspesifikk lovgivning og ulovfestet rett. Man ser også et skille mellom bestemmelser som er knyttet til ivaretakelse av personlige integritet og regler som har fokus på behandling av personopplysninger. I dette kapittelet oppsummeres også noen av svakhetene ved dagens regelverk som Personvernkommisjonen har avdekket ved sin gjennomgang av særskilte områder. Dette er noe kommisjonen mener man bør ha særlig fokus på i forbindelse med revisjon og etterkontroll av regelverket.

2.3 Del III – Det teknologiske landskapet

I *kapittel 9* tar kommisjonen for seg sentrale teknologier og trender, og hvordan disse har innvirkning på personvernet.

I *kapittel 10* drøftes ulike former for personvernfremmende teknologier, og da særlig teknologier for identitetsforvaltning. Kommisjonen viser videre til vedlegg 4 for en ytterligere utdyping av dette.

I *kapittel 11* foreslår kommisjonen følgende:

1. *Ny teknologis innvirkning på personvernet bør utredes.*
   Ved introduksjon av ny teknologi i samfunnet bør som hovedregel teknologiens innvirkning på personvernet utredes på lik linje med teknologiens innvirkning på miljø og økonomi.
2. *Kontinuitet i arbeidet med å kartlegge og formidle teknologiutviklingen.*
   Datatilsynets faglige virksomhet og det arbeidet som gjøres av Teknologirådet med å kartlegge og formidle teknologiutviklingen til politikere og publikum er viktig. Det bør sikres tilstrekkelige ressurser til at begge organers arbeide på dette området fortsetter.
3. *Opprusting av kryptokompetanse.*
   Det bør bli en prioritert offentlig oppgave å ruste opp brukermiljøer som håndterer personopplysninger i riktig og effektiv bruk av kryptering.
4. *Arbeidet med PKI bør intensiveres*
   Det pågående arbeidet med infrastruktur for distribusjon av offentlige kryptografiske nøkler bør intensiveres.

2.4 Del IV – Særskilte områder kommisjonen har arbeidet med

I Personvernkommisjonens mandat var det fremhevet noen konkrete områder/sektorer hvor regjeringen mente at personvernutfordringene er mange og vanskelige. Kommisjonen ble derfor bedt om å ha særskilt fokus på spørsmål som gjaldt personvern i helsesektoren, personvern i samferdselssektoren, personvern i arbeidslivet, personvern og media, samt personvern for barn og unge. I rapportens del IV presenteres Personvernkommisjonens observasjoner og forslag til tiltak innenfor de ovennevnte områdene

2.4.1 Personvern og media

Forholdet mellom to sentrale menneskerettigheter, personvern og ytringsfrihet, står ofte sentralt i debatten om hvordan mediene fungerer i vårt samfunn. I noen situasjoner kan ytringsfriheten være i konflikt med personvernet. I andre tilfeller er ytringsfriheten en forutsetning for personvernet.

Dette spennings- og samvirkeforholdet blir drøftet i *kapittel 13*, som tar for seg personvernet i forhold til mediene. Særlig går kommisjonen inn på digitale media og media med deltagerstyrt innhold og hva disse innebærer i forhold til ansvar, regulering, medietyper og medieroller.

Personvernkommisjonen fremhever særlig følgende åtte forslag til tiltak med sikte på å styrke personvernet i forhold til mediene:

1. *Medieansvarslov.*
   Personvernkommisjonen foreslår at Ytringsfrihetskommisjonens forslag fra 1999 om en egen medieansvarslov følges opp. En slik medieansvarslov bør omfatte alle media, og klargjøre hvem som er ansvarlig i media som er uten redaktør.
2. *Fotografering, og retten til eget bilde.*
   Personvernkommisjonen foreslår at man i samband med den kommende revisjon av åndsverkloven vurderer hvordan bestemmelsen i åndsverkloven om retten til eget bilde er å forstå i forhold til øvrige lovbestemmelser og avveiningen mellom Den europeiske menneskerettighetskonvensjonen artikkel 8 og 10.
3. *Utvidelse av fri rettshjelpordningen.*
   Personvernkommisjonen foreslår at fri rettshjelpsordningen utvides til å omfatte saker mot mediene.
4. *Organ for nettytringer.*
   Personvernkommisjonen foreslår at det opprettes et eget organ som kan bidra til å utvikle gode etiske retningslinjer for nettytringer, og respondere på og løse ulike konflikter som ikke faller inn under andre organers myndighetsområder eller PFU sitt arbeidsfelt.
5. *Slettehjelp.*
   Personvernkommisjonen foreslår at det opprettes en tjeneste som kan bistå de som får sitt personvern krenket på Internett. Denne tjenesten skal ha som oppgave å identifisere og oppnå kontakt med den som er ansvarlig for publiseringen og bistå ved bruk av selvbetjente slettetjenester.

6. *Offentliggjøring av skattelistene.*
   Personvernkommisjonen er delt i synet på offentliggjøring av skattelistene. Flertallet mener det er viktig av hensyn til samfunnsdebatten at skattelistene er tilgjengelig for publikum. For å hindre misbruk bør slik tilgang både for publikum og mediene kun skje på Skatteetatens nettsider, og mulighetene til søk og sammenstilling av opplysninger bør være begrenset. To medlemmer har kommet med særuttalelser. Ett medlem ønsker at skattelistene ikke skal være tilgjengelig. Ett medlem ønsker å opprettholde dagens ordning der redaksjonene kan bruke skatteopplysninger til å drive journalistisk arbeid ved å bearbeide og analysere lett tilgjengelige data.
7. *Pliktavlevering av elektronisk materiale.*
   Personvernkommisjonen mener at personvernhensyn ikke er godt nok tatt vare på i planen for pliktavlevering av elektronisk materiale som er under utvikling i Nasjonalbiblioteket, og foreslår tre konkrete tiltak for å bøte på dette.
8. *Internasjonalisering av nettregulering.*
   Personvernkommisjonen mener at Norge bør være en aktiv pådriver for at regulatoriske tiltak som kan styrke personvernet på nettet spilles inn i relevante internasjonale fora der Norge deltar, med tanke på internasjonalisering og samordning av nettregulering.

2.4.2 Personvern for barn og unge

Barn og unge tar raskt i bruk ny teknologi og er uredde, og til tider ukritiske, i sin anvendelse av denne. Særlig gjelder dette bruk av nye media som er innrettet på publisering av informasjon om en selv eller andre. Samtidig har ikke alltid barn tilstrekkelig erfaring eller kunnskap til å se konsekvensene av slik offentliggjøring. Barn er også ofte prisgitt foresattes eller andre voksnes beslutninger og tiltak som kan få betydning for deres personvern, for eksempel i forhold til publisering av bilder eller bruk av teknologiske verktøy.

I *kapittel 14* behandles spørsmålet om personvern for barn og unge. Selv om de øvrige temaene som diskuteres i rapporten også er relevante for denne gruppen, er det grunn til å ha et særskilt fokus på personvernproblemstillinger som berører barn og unge spesielt.

Personvernkommisjonen observerer at for barn og unge er det å publisere bilder og opplysninger om seg selv eller andre blitt en naturlig del av måten å kommunisere på. Nettet er imidlertid ikke bare en arena for sosialisering, nettverksbygging og meningsytring, men også for konfliktskapning, ryktespredning, trusler og mobbing. Barn og unge må bevisstgjøres i forhold til hvor alvorlig det er å legge ut informasjon som kan skade deres eget og andres omdømme og personlige integritet. Digital mobbing er et stadig økende problem, og kan ofte føles mer alvorlig enn tradisjonell mobbing. Særlig fordi rykter, usanne og krenkende påstander på for eksempel Internett er nærmest irreversibelt, noe som fører til at krenkelsen vedvarer.

En annen problemstilling som har vært sentral i kommisjonens arbeid er foreldres publisering av bilder og personopplysninger om egne barn på Internett. Vanligvis skjer dette i uskyldige former og innenfor forsvarlige rammer, slik at personvernet blir ivaretatt. Flere offentlige etater advarer imidlertid mot å legge ut bilder av barna på nett. Det finnes også flere eksempler på at foreldre publiserer svært utleverende materiale om barna sine, samtidig som det synes usikkert hvor grensene for dette går rent juridisk.

Personvernkommisjonen har også vært oppmerksomme på ulike problemstillinger som gjelder personvern i skolesektoren. Nye digitale læringsformer, omfattende digital datainnsamling, samt bearbeiding og bruk av disse, stiller utdanningssystemet overfor personvernmessige utfordringer, både med hensyn til hvilke typer opplysninger som gjøres tilgjengelig og hvilke sikkerhetsmessige tiltak som iverksettes. Disse utfordringene har til nå ikke vært viet stor oppmerksomhet, verken på skole eller administrativt nivå. Det blir mer og mer vanlig å iverksette ulike former for overvåkning av skoleelever, for eksempel kameraovervåkning i skolegården og PC-overvåkning. Det er tydelig for kommisjonen at man er mindre bevisst når det gjelder å innføre personverninngripende tiltak overfor barn enn man ville vært på en arbeidsplass, selv om skolen på mange måter må anses som barns arbeidsplass.

I forhold til de observasjonene som er gjort, foreslår Personvernkommisjonen følgende tiltak for å imøtekomme de utfordringene barn og unges personvern står overfor:

1. *Tiltak for å trygge barn og unges rettsikkerhet og personvern.*
   Kommisjonens mener å ha identifisert klare svakheter ved dagens rettslige regulering i forhold til spørsmålet om samtykkekompetanse. Særlig gjelder dette foreldrenes rett til å samtykke på vegne av barna til publisering av personopplysninger, selv om barnets rett til inte-

gritet og personvern kunne tilsi at slik publisering ikke fant sted. Kommisjonen foreslår at det utredes nærmere hvorvidt denne typen behandling av personopplysninger bør ilegges restriksjoner slik at samtykke etter personopplysningsloven § 8 (eventuelt § 9) ikke utgjør et tilstrekkelig behandlingsgrunnlag.

2. *Styrking av personvernet ved bruk av digitale media.*
   I kapittelet om personvern og media foreslår Personvernkommisjonen flere tiltak som skal bidra til å styrke personvernet i forhold til mediene, og særlig når det gjelder såkalte «nye media». Disse forslagene berører i høyeste grad ivaretakelsen av barn og unges personvern. Eksempelvis forslås det at det opprettes et organ som skal løse konflikter knyttet til ytringer på Internett, herunder digital mobbing. Videre mener Personvernkommisjonen at det må vedtas en medieansvarslov som definerer hvem som er ansvarlig for personvernkrenkelser på nett. Et klart ansvarssubjekt vil antagelig medvirke til at regler som gjelder aldersgrenser og samtykke fra barn i større grad blir etterlevd.
3. *Personvernansvarlig i skolen.*
   Personvernkommisjonen foreslår at hver skole har en ansatt med spesiell kunnskap om personvern og personopplysningsloven. Skolens personvernressurs kan ha som oppgave å bistå elever med å ivareta sine rettigheter, bistå i arbeidet med å skape gode rutiner for behandling av personopplysninger internt i virksomheten, påpeke brudd på regler om behandling av personopplysninger samt holde seg orientert om utviklingen på personvernområdet. I tilegg kan en slik person gi råd og veiledning til elever, lærere og foreldre i spørsmål som angår personvern. For ytterligere å styrke skolenes kompetanse på området, vil Personvernkommisjonen også anbefale at spisskompetanse om personvernforhold finnes hos sentrale utdanningsmyndigheter
4. *Synlige etater på nettet.*
   Ettersom nettet er en viktig sosial arena for barn og unge mener Personvernkommisjonen det er viktig at offentlige etater er synlig tilstede på sosiale nettarenaer som er populære blant barn og unge. Her kan de rettlede, veilede og informere barn og unge om rettigheter og plikter.
5. *Opplysningsarbeid og annet holdningsskapende arbeid.*
   Personvernkommisjonen mener skolen har et særlig ansvar når det gjelder å formidle informasjon om rettigheter og plikter angående personvern, og skape gode holdninger som kan ligge til grunn for en moralsk forsvarlig bruk av den digitale dømmekraften. Skolen har også et ansvar for å bidra til at personvernet blir likt fordelt. Skolen må informere barn og unge om de rettighetene de selv har og om hvilke plikter de har overfor andre. Dette kan også være en del av skole/hjem samarbeidet.
6. *Delta på arenaer der det er mulig å påvirke internasjonale regler.*
   Mye av det som utfordrer barn og unges personvern kan ikke reguleres gjennom nasjonal lovgivning. Derfor er det viktig at norske myndigheter deltar på arenaer der det er mulig å påvirke utviklingen av internasjonale regler. For å beskytte personvernet til barn og unge er det særlig viktig å arbeide for felles retningslinjer med hensyn til aldersgrenser og samtykke.

2.4.3 Personvern i arbeidslivet

Både arbeidslivet og næringslivet preges av store endringer. Utvikling og bruk av ny teknologi, endrede konkurranseforhold, demografisk utvikling, økt utdanningsnivå samt globalisering og internasjonalisering er viktige faktorer.

Personvernkommisjonen har notert seg at organiseringen av arbeidet og arbeidsformer endres, og da særlig som en følge av at informasjonsteknologien endrer arbeidsprosesser og -oppgaver. Dette har fått flere følger for arbeidstakeres personvern. Den teknologiske utviklingen gjør det svært enkelt å overvåke både ansatte, kunder og andre som kan relateres til en virksomhet, og utviklingstrekkene i arbeidslivet gjør at man finner stadig nye begrunnelser for økt overvåkning. Økt informasjonsvolum i arbeidslivet i form av ulike former for elektroniske spor, kommunikasjonsdata, elektronisk lagrede virksomhetsopplysninger og opplysninger om ansatte, vil generelt innebære at det innsamles mer opplysninger om den ansatte og følgelig en økt risiko for lekkasje av opplysninger til uvedkommende

I *kapittel 15* har Personvernkommisjonen valgt å fokusere på overvåkning i arbeidslivet som en hovedproblemstilling innenfor temaet personvern i arbeidslivet. Fokuset er rettet mot arbeidsgivers innsyn i ansattes e-post, da dette gir et godt bilde av de utfordringene som oppstår i avveiningen mellom arbeidsgivers interesser og arbeidstakeres interesser. I kapittelet berøres også varslingsreglene i arbeidsretten.

Personvernkommisjonen observerer at nivået og omfanget av overvåkning i arbeidslivet synes å

ha økt betydelig de siste årene. Tilgjengeligheten av ny teknologi forbundet med lave kostnader gjør terskelen lav for iverksetting av systemer som direkte eller indirekte kan sies å innebære kontrolltiltak overfor ansatte. Det kan være alt fra adgangskontroll til avlytting av telefonsamtaler og kartlegging av ansattes nettverk. Det har også blitt vanligere at private aktører tar i bruk «politimetoder» for å avdekke mislighold blant egne ansatte. Eksempler på dette er bruk av skjult kameraovervåkning og fremleggelse av bilder fra overvåkning som bevis mot arbeidstakere. Personvernkommisjonen mener at det å bli overvåket i sitt daglige virke vil oppfattes som en belastning av de fleste. Dersom opplysningene som innhentes ved slik overvåkning i tillegg blir brukt til andre formål enn de opprinnelig var beregnet for, og andre formål enn dem man har fått informasjon om, øker dette belastningen og følelsen av overtramp mot den personlige integritet.

I dette kapittelet fremhever Personvernkommisjonen derfor noen grunnleggende retningslinjer for overvåkning på arbeidsplassen.

Når det gjelder innsyn i e-post, ser Personvernkommisjonen at det må foretas vanskelige avveininger mellom arbeidstakers personvern og arbeidsgivers legitime interesse/behov for innsyn og kontroll. Informasjon, åpenhet og gjennom dette, forutsigbarhet for begge parter, fremheves som svært viktig. Personvernkommisjonen knytter også noen generelle kommentarer til det pågående arbeidet med å fastsette forskrifter om arbeidsgivers rett til innsyn i ansattes e-post.

Kommisjonen erfarer at det er et problem at reglene for personvern og integritetsvern i arbeidslivet er spredt over forskjellige lover og rettsområder. Dette er en utfordring i forhold til følelsen av «eierskap til regelverket», noe som igjen får konsekvenser for etterlevelse av det gjeldende regelverket. Kommisjonen etterlyser derfor et helhetlig regelverk som tydelig angir grensene for arbeidssøkere og arbeidstakeres integritetsvern, personvern og personopplysningsvern. Lovgiver bør søke å få på plass et regelverk som partene i arbeidslivet er enige om, og hvor den nødvendige balansen mellom arbeidsgivers og arbeidstakers interesser er synliggjort. Et hensiktsmessig og godt balansert regelverk vil etter kommisjonens oppfatning være med på å sikre etterlevelse fra partenes side.

Kommisjonen anbefaler videre at det iverksettes tiltak som øker bevisstheten rundt personvern i arbeidslivet, rettet både mot arbeidsgiversiden og arbeidstakersiden. Personvernkommisjonen anbefaler også at man får økt fokus på styrking av personvernkompetansen i arbeidslivet, for eksempel ved å presisere at verneombudets funksjon også omfatter personvernspørsmål.

2.4.4 Personvern i helsesektoren

Helsetjenesten er avhengig av tilgang på helseopplysninger for å kunne gi pasientene forsvarlig og individuelt tilpasset helsehjelp. Helsetjenesten skal også løse mange andre oppgaver og er under et konstant press med tanke på både å gjøre mer (behandle flere), forbedre tjenestetilbudet (ta i bruk ny kunnskap og nye metoder, øke kvaliteten, fremme sikkerhet) og sørge for at de er kostnadseffektive. Samtidig er personopplysninger om helseforhold og sosiale omstendigheter blant de mest private og sensitive, og det er derfor viktig at disse er godt beskyttet både rettslig og i praksis. I Personvernkommisjonens mandat pekes det nettopp på at helsesektoren er ett av flere områder der personvernutfordringene er mange og vanskelige.

Personvern i helsesektoren behandles i rapportens *kapittel 16*. Fokuset er særlig rettet mot personvernspørsmål som følger i kjølvannet av elektronisk pasientjournal, samarbeid og informasjonsutveksling av pasientopplysninger, både internt i helsetjenesten og på tvers av virksomheter, samt opprettelsen og bruk av helseregistre.

I dette kapittelet drøfter Personvernkommisjonen den lovbestemte taushetsplikten som påhviler alt helsepersonell og hvordan denne er under konstant press. Unntakene er etter hvert mange, og strømmen av helseopplysninger som med lovgivers tillatelse går til ulike faglige og administrative instanser er stor og økende. I tillegg kan det synes som om helsepersonell i altfor stor grad kommuniserer helseopplysninger i strid med taushetsplikten, enten på grunn av manglende kunnskap om regelverket eller på grunn av manglende respekt for dette. Det at pasientdata både er lettere og mer tilgjengelige i dagens elektroniske systemer, har medført en økning i personvernrisikoen i helsesektoren.

Personvernkommisjonen observerer også økt press på tilgang til pasientdata, både internt i virksomheter og på tvers av virksomheter, uten at det er tilfredsstillende dokumentert at personvernhensyn ivaretas. Personvernkommisjonen mener at mye av tilgangen som gis til direkte identifiserbare data per i dag er unødvendig, og at både kontrolloppgaver og administrative oppgaver kunne vært gjennomført uten individualiserende kjenne-

tegn. Personvernkommisjonen drøfter NAV-reformen som et eksempel på samarbeid og informasjonsutveksling hvor personvernet settes på prøve.

Personvernkommisjonen observerer videre at praksisen knyttet til opprettelsen av helseregistre reiser mange og vanskelige personvernspørsmål. Det etablerers mange og sensitive registre som møter massiv personvernfaglig kritikk fra sentrale miljøer. Dette er i seg selv en utfordring. Personvernkommisjonen fremhever Norsk pasientregister og IPLOS som to eksempler her.

I forhold til de observasjoner som er gjort har Personvernkommisjonen følgende forslag til tiltak for bedre å ivareta personvernet i helsesektoren:

1. *Kommunikasjon med pasienter.*
   Det må innføres nye rutiner for å sikre retten til at sensitive helseopplysninger ikke formidles i påhør av andre. Også pasienter som ligger på rom med flere har krav på taushet om sine personlige forhold. Den tradisjonelle legevisitten bør reformeres på en slik måte at taushetsplikten ivaretas.
2. *Utelatelse av individualiserende kjennetegn.*
   Det bør gjennomføres tiltak for å sikre at personvernhensyn ivaretas i tråd med lovgivers intensjoner når opplysninger eller journalutdrag brukes i samband med internkontroll. De tekniske mulighetene elektronisk pasientjournal (EPJ) faktisk gir for pseudonymisering og andre metoder for å skjule identitet bør utnyttes fullt ut. Standarden for EPJ bør utvikles slik at individualiserende kjennetegn ved enkle grep kan erstattes med automatisk genererte pseudonymer. Klageinstanser i helsesektoren, inklusive Helsetilsynet, bør gå gjennom sin praksis i forhold til å utelate identifiserende kjennetegn i klagesaker, og i denne forbindelse vurdere tiltak for immunisering av søkemotorer.
3. *System for identitetsadministrasjon.*
   Som en videreutvikling av tiltak for automatisk pseudonymisering av individualiserende kjennetegn, kan det være aktuelt å knytte slik pseudonymisering til et system for identitetsadministrasjon.
4. *Personvernvennlig bruk av elektronisk pasientjournal (EPJ).*
   Det er nødvendig med personvernfremmende tiltak både med tanke på utvikling av tilfredsstillende programvare, rutiner og annet av betydning for faktisk etterlevelse av taushetsplikten. Mulighetene for tekniske og menneskelige feil må begrenses og IKT-bruken må tilpasses helsetjenestens krav, ikke minst bestemmelsene om taushetsplikt og behovet for tilgangskontroll. Det er behov for en grundig gjennomgang av personvernhensyn før det gis tilgang til EPJ på tvers av foretak. Det må sørges for ivaretakelse av taushetsplikt og personvernhensyn før det kan åpnes for eksternt innsyn i pasientjournaler.
5. *Gjennomgang av reglene for taushetsplikt.*
   Personvernkommisjonen vil anbefale at bestemmelsene om taushetsplikt gjennomgås med tanke på å evaluere hvorvidt dagens regelverk samlet sett innebærer en tilstrekkelig ivaretakelse av sentrale personvernhensyn.
6. *Forbedring av pasienters rett til innsyn i journallogg.*
   Personvernkommisjonen støtter forslaget om at retten til innsyn i tilgangsloggen til pasientjournalen lovfestes. Det bør videre stilles konkrete krav til hva loggen skal inneholde, og den må være skrevet på en slik måte at pasienten selv kan forstå hvem det er som har vært pålogget journalen, når påloggingen er gjort, begrunnelsen for påloggingen og hvilke aktiviteter den påloggede har utført.
7. *Opplærings- og holdningsskapende tiltak, innføring av bedre rutiner.*
   Personvernkommisjonen mener det foreligger et klart behov for systematiske opplærings- og holdningsskapende tiltak og bedrede rutiner for å sørge for at taushetsplikten etterleves i praksis. Det er svært viktig at helsepersonell gis grundig opplæring i reglene om taushetsplikt, ikke minst bestemmelsen i helsepersonelloven § 25, 1. ledd om at det bare kan gis opplysninger til samarbeidende helsepersonell og bare i den grad dette er nødvendig for å kunne gi forsvarlig helsehjelp. Personvernkommisjonen tror at et enda større fokus på taushetsplikt og personvern i grunnutdanningen for personell i helse- og sosialsektoren vil være et effektivt virkemiddel i denne sammenheng.
8. *Personvernfremmende tiltak ved opprettelsen av nye registre.*
   Det bør foretas grundige utredninger før nye helseregistre etableres. Det er ikke tilstrekkelig at registeret kan sies å tjene et godt formål. Konsekvensene for personvernet må utredes bedre, og det må kunne dokumenteres at disse ikke er så negative at man av den grunn bør avstår fra å opprette registeret. Det må også tilstrebes å gjøre bruken av registeret så personvernvennlig som mulig, for eksempel gjennom pseudonymisering eller andre metoder for

identitetsbeskyttelse. Ethvert register bør også undergis periodisk ettersyn og en revurdering, som bør være bygget inn i betingelsene for registerets rettslige grunnlag. Ved jevne mellomrom bør registeret opp til ny vurdering, der balansen mellom personvernet og andre interesser revurderes før hjemmel for registeret eventuelt forlenges.

9. *Gjennomgang av dagens helseregistre.*
   Personvernkommisjonen foreslår en gjennomgang av alle etablerte sentrale helseregistre, med et klart fokus på personvern. Det bør foretas en utredning av hvorvidt de eksisterende registrene har en berettiget eksistens og om det finnes registre med overlappende funksjon og formål. Det bør også vurderes om ikke pseudonymisering er et tiltak som kan tas i bruk for langt flere helseregistre enn det som er tilfelle i dag. Kommisjonen foreslår at det vedtas et moratorium mot etablering av nye helseregistre før denne gjennomgangen er fullført.

2.4.5 Personvern i samferdselssektoren

Samferdsel handler om måter å oppnå kontakt mellom mennesker på, enten gjennom fysisk forflytning ved hjelp av bil, tog, båt, fly mv. (transport), eller ved media som overfører informasjon, som post, telefon og Internett (kommunikasjon).

Personvern i samferdselssektoren drøftes i *kapittel 17*, der kommisjonen særlig ser på tiltak som er rettet inn mot sikkerhetshensyn, ettersom det særlig er tiltak begrunnet i sikkerhetshensyn som setter personvernet under press. Med «sikkerhet» siktes det her til vern mot bevisste handlinger som har til hensikt å gjøre skade («security») og vern mot skade som er utilsiktet («safety»).

I dette kapittelet observerer kommisjonen at nye regimer for elektronisk lagring av trafikkdata er en utfordring for personvernet. I denne forbindelse drøfter Personvernkommisjonen det såkalte datalagringsdirektivet (2006/24/EF). Uttalelsen er basert på selve direktivteksten, da forslaget om innføring av direktivet i norsk rett ikke var fremlagt i skrivende stund.

Kommisjonen viser blant annet til at det må foretas en grundig utredning av konsekvensene for personvernet både om direktivet blir innført i norsk rett eller ikke.

Kommisjonen etterlyser videre en grundigere klargjøring i form av dokumentasjon av behovet for lagring, både lagringstid og omfang av opplysninger, og en grundig konsekvensutredning. I denne sammenheng viser kommisjonen til dokumentasjonskravet som følger av artikkel 8 i EMK.

Personvernkommisjonens konklusjon er at de ikke kan støtte innføring av direktivet uten at behovet for utvidet lagring er bedre dokumentert.

Personvernkommisjonen drøftet og ga en særlig uttalelse om datalagringsdirektivet i juni 2008. Denne ligger som vedlegg til rapporten.

Personvernkommisjonen har fremmet fem forslag til tiltak for bedre å ivareta personvernet i samferdselssektoren:

1. *Økt vektlegging av kravet om proporsjonalitet.*
   Kravet følger allerede av sentrale deler av personvernregelverket, men det må vektlegges og synliggjøres bedre. Proporsjonalitetskravet bør være særlig sentralt i forhold til en eventuell innpasning av EUs datalagringsdirektiv eller tilsvarende i norsk rett.
2. *Sporfrie og/eller anonyme løsninger.*
   Det bør legges til rette for sporfrie og/eller anonyme løsninger i forhold til betaling og bruk av transporttjenester. Grunnregelen bør være at når en tilbyr et elektronisk billettsystem eller lignende, skal det være mulig å benytte seg av et sporfritt alternativ.
3. *Automatisert registrering som er integrert i produkter må gjøres synlig.*
   Det bør gjøres en systematisk innsats for å synliggjøre overfor befolkningen de nye formene for registrering og regelbaserte systemer som i tiltakende grad integreres i produkter og omgivelser. Det bør videre utredes hvordan nåværende regelverk løser spørsmål knyttet til eierskap og bruk av data som registreres i slike systemer, og hvorvidt regelverket bør endres til bedre å fremme personvernhensyn ved produksjon og bruk av slike data.
4. *Begrensninger på bruk av automatisk registrering.*
   Bortsett fra i begrenset omfang rettet mot yrkesmessig transport, bør det ikke være adgang til å innføre eller benytte automatiske registreringssystemer i alminnelige produkter der hensikten med registreringen er å ha en disiplinerende funksjon overfor den som bruker produkter.
5. *Fortsatt liberal kryptopolitikk.*
   Staten bør fremdeles ta avstand fra innføring av obligatorisk deponering av kryptografiske nøkler som innehas av privatpersoner. Staten bør videre vise stor forsiktighet ved å innføre begrensninger på folks rett til å ta i bruk sterk kryptering.

2.5 Del V – Andre områder kommisjonen har arbeidet med

2.5.1 Organisering av personvernmyndighetene

Som ledd i å kartlegge og evaluere de virkemidlene som eksisterer for å ta vare på personvernet i Norge, drøfter Personvernkommisjonen organiseringen av Datatilsynet og Personvernnemnda i *kapittel 18*.

Personvernkommisjonen har observert at Datatilsynet har svært mange og vidtspennende oppgaver, fra stedlig tilsyns- og kontrollvirksomhet, rådgiving, generell informasjonsvirksomhet og deltagelse i samfunnsdebatten, til faglig virksomhet og deltagelse i internasjonale fora for å ivareta egen og samfunnets kompetanse på området personvern og personopplysningsvern. Datatilsynet er således et tilsynsorgan i tillegg til at de påtar seg rollen som «personvernets ombudsmann».

Personvernkommisjonen mener at ombudsfunksjonen er viktig og at personvernet i møte med andre interesser trenger noen som taler personvernets sak og som tør å kritisere både offentlige myndigheter og private aktører når de på ulike måter utfordrer personvernet.

Personvernkommisjonen mener likevel at det kan være problematisk at det forvaltningsorganet som treffer enkeltvedtak og utøver myndighet etter personopplysningsloven, er det samme organet som er gitt i oppgave å tale personvernets sak. Den konkrete myndighetsutøvelsen etter personopplysningsloven forutsetter en avveining av mange ulike interesser og det kan i noen tilfeller være uheldig at avveiningen foretas av et organ som oppfatter at deres oppgave er å ivareta én spesiell interesse fremfor en annen. I denne sammenheng fremhever kommisjonen at Personvernnemnda er et kollegialt organ satt sammen av personer med ulik bakgrunn nettopp for å sikre en bred interesse- og fagrepresentasjon.

Et flertall i Personvernkommisjonen mener likevel at Datatilsynet bør videreføre sine arbeidsområder med oppgaver som kombinerer tilsyns- og ombudsvirksomhet. Et mindretall (1 medlem) anbefaler et organisatorisk skille mellom tilsynsoppgaver og ombudsoppgaver.

Når det gjelder fremtidig organisering av personvernmyndighetene forslår Personvernkommisjonen følgende tiltak:

1. *Økte ressurser til Datatilsynet.*
   Datatilsynet bør få tilført flere ressurser til sin virksomhet. Teknologiutviklingen og utbredelsen av nye media vil i tiden som kommer utfordre personvernet, men også skape muligheter for et bedre personvern og et sterkere personopplysningsvern. For å møte disse utfordringene og ivareta teknologiske muligheter, mener Personvernkommisjonen at man må ha et særlig fokus på hvordan Datatilsynets kompetanse og kapasitet sikres og styrkes i forhold til dette.
2. *Regionalisering av Datatilsynet.*
   Personvernkommisjonen anbefaler at en vesentlig del av ressursøkningen i Datatilsynet skjer gjennom regionalisering. Lokale kontorer kan ha et særlig ansvar for gjennomføring av tilsyn innenfor sin region, behandling av meldinger om installering av overvåkningskameraer, oppfølging av lokale personvernombud, lokal rådgivings- og informasjonsvirksomhet etc.
3. *Et råd for Datatilsynet.*
   Personvernkommisjonen mener at det bør opprettes et «Datatilsynets råd» som kan fungere som et kollegialt rådgivingsorgan med en bred sammensatt kompetanse. Rådets mandat bør være knyttet til særlig vanskelige og prinsipielle saker og klagesaker.
4. *Sektorvis styrking av personvernkompetansen.*
   Personvernkommisjonen anbefaler at også andre forvaltningsorganer som kommer i berøring med personvernproblemer (som for eksempel Arbeidstilsynet, Helsetilsynet og Utdanningsdirektoratet) sikrer at de har en person internt med høy personvernfaglig kompetanse og da særlig i forhold til personvernspørsmål som er relevante for dette organet.
5. *Samarbeide med eksterne aktører.*
   Personvernkommisjonen anbefaler at Datatilsynet fortsetter å samarbeide med andre aktører for å nå fram til publikum med informasjons- og holdningsskapende arbeid.
6. *Dialog med akademia og andre fagmiljøer.*
   Datatilsynet bør sørge for løpende kontakt med akademia (universiteter, høyskoler og forskningsinstitusjoner). Dette vil bidra til å øke oppmerksomheten hos ansatte i disse institusjonene omkring personvernspørsmål, samt utgjøre et grunnlag for gjensidig kompetanseoverføring mellom Datatilsynet og akademia.

2.5.2 Grunnlovsfesting av personvernet

Grunnlovsfesting av personvernet er et viktig politisk tema og har lenge vært en del av den offentlige debatten. I *kapittel 19* diskuterer Personvernkommisjonen hvorvidt personvernet bør grunnlovsfestes i Norge.

Grunnloven har stor rettslig og politisk betydning, i tillegg til at den har en vesentlig symboleffekt både for borgerne og staten. Personvernkommisjonen mener at grunnlovsfesting av personvernet vil medføre at personvernet får en sentral rolle i konkrete saksforhold, samtidig som man presiserer at også individuelle rettigheter er en viktig del av vår rettstat. Personvernkommisjonen påpeker videre at en grunnlovsfesting av personvernet vil kunne styrke vektleggingen av personverninteresser når man vedtar nye lover og i lovgivningsprosessen. Det fremheves også at grunnlovsfesting av personvernet vil skape bedre balanse mellom ytringsfrihet og personvern, da dette er to interesser som ofte står i et motsetningsforhold.

Personvernkommisjonen anbefaler at personvernet, herunder retten til privatliv og personopplysningsvernet grunnlovsfestes i Norge.

Kapittel 3
Økonomiske og administrative konsekvenser

De tiltak som Personvernkommisjonen foreslår, og som er oppsummert i kapittel 2, vil i ett tilfelle gi økt proveny, men vil i mange tilfeller kreve midler til drift, prosjektgjennomføring eller utredning. Andre tiltak vil kreve at det bevilges midler til kompetanseheving, eller at det gjennomføres administrative grep.

3.1 Tiltak som vil gi økt proveny

Kommisjonen foreslår å legge avgifter på enkelte tiltak som kan ha negativ effekt på personvernet, for eksempel kameraovervåkning. Dette vil gi inntekter som for eksempel kan benyttes til å styrke Datatilsynet.

3.2 Tiltak som er betinget av midler til drift, prosjektarbeide eller utredning

- For å sørge for kontinuitet i arbeidet med å kartlegge og formidle teknologiutviklingen må Teknologirådet få tilført de ressurser rådet trenger for å ivareta disse oppgavene. Datatilsynet bør av samme grunn få økte ressurser, se nedenfor.
- Det pågående arbeidet med PKI ser ut til å ha dårlig fremdrift. En tilførsel av ressurser og midler synes nødvendig, slik at offentlig sektor, gjerne i samarbeid med private leverandører av egnet teknologi, kan prioritere denne oppgaven.
- En medieansvarslov, slik Personvernkommisjonen i likhet med Ytringsfrihetskommisjonen foreslår, forutsetter et offentlig utredningsarbeid.
- En utvidelse av fri rettshjelpordningen til å omfatte saker mot pressen vil gi økte utgifter. Det må også utredes nærmere hva som skal være kriteriene for å omfattes av ordningen.
- Opprettelse av et organ for tvisteløsning i forbindelse med krenkende ytringer på Internett, vil kreve finansiering. Flere finansieringsmodeller, inklusive brukerfinansiering, er mulig. Personvernkommisjonen primære forslag er imidlertid at organet blir offentlig finansiert.
- Forslaget om slettehjelp vil kunne realiseres ved at oppgavene legges til en eksisterende etat, for eksempel Post- og Teletilsynet. Behovet er neppe større enn at oppgaven vil kunne gjennomføres innenfor 20 % av et årsverk.
- Økt norsk aktivitet i internasjonale fora for nettregulering med særlig henblikk på å styrke internasjonalt samarbeid og regulering foreslås, både når det gjelder personvern i nye media, og i forhold til barn og unges personvern. Slik deltagelse vil kreve en innsats fra de organer som deltar på slike arenaer, i første rekke Barneombudet, Post- og Teletilsynet, og Datatilsynet. Personvernkommisjonen har ikke kunne tatt stilling til om dette er gjennomførbart med de midler disse etatene disponerer til internasjonal virksomhet per i dag, eller om det kreves ytterligere bevilgninger.
- Synlige etater på nettet vil kreve at relevante etater bruker mer ressurser på slik tilstedeværelse.
- Tiltakene som retter seg mot Nasjonalbibliotekets innsamling av elektronisk materiale medfører at det må foretas en utredning og gjennomgang av dagens regulering.
- Opplysningsarbeid og annet holdningsskapende arbeid om personvern rettet mot barn og unge, partene i arbeidslivet, og på andre arenaer, vil sannsynligvis skape behov for økte ressurser.
- Utelatelse av individualiserende kjennetegn i EPJ vil sannsynligvis kreve en viss oppgradering av programvare for EPJ, noe som vil medføre kostnader.
- System for identitetsadministrasjon vil sannsynligvis kreve et større utviklingsprosjekt for å designe og utvikle et hensiktsmessig datasystem som støtter dette.

- Å få på plass mer personvernvennlig bruk av EPJ vil kreve innsats med hensyn til organisasjonsutvikling i helsesektoren.
- En gjennomgang av reglene for taushetsplikt er betinget av prosjektmidler.
- En gjennomgang av dagens helseregistre vil kreve et større utredningsarbeid.
- Utredning av rekkevidden av dagens regelverk knyttet til eierskap og bruk av data som skaffes til veie ved automatisk registrering som er integrert i produkter vil kreve prosjektmidler.
- Økte ressurser til Datatilsynet, blant annet for å muliggjøre regionalisering, økt internasjonal deltagelse, mer samarbeide med eksterne aktører og tettere dialog med akademia og andre fagmiljøer, innebærer et betydelig økonomisk løft. Personvernkommisjonen anslår behovet til om lag 25 årsverk, fordelt på fem regionale kontorer.
- Opprettelse av et kollegialt råd for Datatilsynet innebærer at det må oppnevnes medlemmer og bevilges penger til honorar for møtedeltagelse
- En grunnlovfesting av personvernet forutsetter at det gjennomføres et større utredningsarbeid.

3.3 Tiltak som krever kompetanseheving

- Opprusting av kryptokompetanse vil kreve at det bevilges midler til opplæring av de berørte brukermiljøer i bruk av kryptografi, til programvare som kan brukes til kryptering, og til planlegging og gjennomføring av et slikt opprustingsprogram.
- Innføring av en personvernansvarlig i skolen og sektorvis styrking av personvernkompetansen er betinget at den/de ansvarlige tilføres nødvendig kompetanse.
- Innføring av nye rutiner for kommunikasjon med pasienter og bedre rutiner for at taushetsplikten etterleves i praksis, bør skje i samband med generell kompetanseoppbygging omkring yrkesetikk, for eksempel ved kampanjer og opplæring gjennom organisasjonene for de ansatte i helseforetakene.
- En gjennomgang av alle etablerte sentrale helseregistre vil kreve prosjektmidler til et større utredningsarbeid.

3.4 Tiltak med administrative konsekvenser

- Pålegg om å utrede hvilken innvirkning ny teknologi har for personvernet bør reguleres gjennom retningslinjer.
- I samband med den kommende revisjon av åndsverkloven mener kommisjonen at en vurdering av retten til eget bilde bør være en del av mandatet til gruppen som skal arbeide med dette.
- Flertallets forslag, der mediene ikke lenger får direkte tilgang til skattelistene på cd-rom, innebærer at de ressurser som i dag brukes for tilrettelegging av cd-rom-distribusjon, i stedet brukes til tilrettelegging for publisering på skatteetatens egne nettsider.
- Tiltakene som retter seg mot tilgang til innsamlet materiale hos Nasjonalbiblioteket medfører at det må utarbeides nye retningslinjer internt i virksomheten.
- Trygging av barn og unges rettssikkerhet krever en nærmere utredning i forhold til spørsmålet om samtykkekompetanse. Dette bør gjennomføres som ledd i den kommende revisjonen av personopplysningsloven.
- En mer restriktiv praksis ved opprettelsen av nye helseregistre og innføring av personvernfremmende tiltak, vil være betinget av politisk vilje til å innføre en slik praksis. Det samme gjelder for et eventuelt moratorium mot etablering av nye helseregistre før foreslåtte gjennomgang av dagens helseregistre er gjennomført.
- Økt vektlegging av kravet om proporsjonalitet i samband med lovgiving som griper inn i personvernet på samferdselssektoren, forutsetter politisk vilje hos lovgivende myndigheter.
- Tilrettelegging for sporfrie og/eller anonyme løsninger ved betaling for transporttjenester, innebærer i første rekke at det legges sterkere politiske føringer på at slike løsninger skal finnes.
- Synliggjøring av at integrerte produkter automatisk registrer personopplysninger, krever informasjonstiltak overfor forbrukere.
- Begrensninger på bruk av automatisk registrering bør reguleres gjennom lov eller forskrift.

Kapittel 4
Utgangspunkt og avgrensinger

4.1 Nærmere om begrepet personvern

4.1.1 Begrepets fødsel og opprinnelige betydning

Diskursen rundt personvernbegrepet har alltid vært preget av terminologisk uklarhet, forvirring og strid. Dette gjelder ikke bare i Norge; det finnes en skog av akademisk litteratur i USA og andre engelsktalende land der innholdet og nytteverdien av det beslektede «privacy»-begrepet er debattert. For en oversikt, se blant annet Bygrave (2002), kapittel 7.

Allerede på begynnelsen av 1970-tallet kunne Erik Samuelsen – i den første forskningsrapporten som ble skrevet i Norge om personvernmessige problemer knyttet til «statlige databanker» – konstatere:

> «Et typisk trekk ved debatten om de farer som den nye teknologi [sic] representerer for individet, er bruken av en rekke uklare begreper. Det tales om at «privatlivets fred» er i fare. Det påpekes at datamaskinene medfører «inngrep i den personlige integritet». Behovet for «personlighetsvern» understrekes til stadighet. Ofte benyttes også det angloamerikanske uttrykk «privacy» for å angi arten av de interesser som er i faresonen. (Samuelsen 1972, s. 15)»

Tittelen på Samuelsens rapport var «Statlige databanker og personlighetsvern», og refererer altså til «personlighetsvern», ikke «personvern». Sistnevnte begrep er heller ikke brukt i rapporten. Kun kort tid etter rapporten ble utgitt, ble imidlertid «personvern» tatt i bruk som begrep. Dette skjedde i det rettsinformatiske forskningsmiljøet ved Universitetet i Oslo. Begrepet ble i hovedsak brukt som betegnelse på «en mulig interesse fra enkeltpersoners side i å utøve kontroll med den informasjon som beskriver dem» (se Blekeli 1977).

Begrepet ble også raskt tatt i bruk utenfor dette forskningsmiljøet. De to første utvalgene som ble nedsatt av regjeringen til å utrede problemer knyttet til elektronisk behandling av personopplysninger – *Sandvik-utvalget* og *Seip-utvalget* – brukte «personvern» i titlene på sine respektive innstillinger.[1] Det er imidlertid verdt å merke seg at ingen av innstillingene gir noen direkte definisjon av begrepet. Mens Sandvik-utvalget synes å ikke ha tatt definisjonsspørsmålet opp til drøftelse i det hele tatt, avsto Seip-utvalget eksplisitt fra et definisjonsforsøk da det mente at et slikt forsøk ville være vanskelig, relativt nytteløst og lett føre til feil fokus:

> «Både p.g.a. de vanskeligheter som er forbundet med å gi presise og meningsfylte definisjoner og fordi nytteverdien av begrepsbestemmelser på dette felt er svært begrenset, har utvalget funnet at det er lite vunnet ved å definere begreper som personlig integritet, privat rettsfære o.l. ved vurderingen av de problemer som kan oppstå for enkeltpersoner ved bruk av EDB. Etter utvalgets oppfatning vil et slikt utgangspunkt også lett føre til en for ensidig konsentrasjon om de negative sider ved de nye tekniske hjelpemidler for behandling av data (NOU 1975:10, side 12).»

Datatilsynet tok også personvernbegrepet raskt i bruk og la til grunn følgende definisjon av begrepet i sin årsmelding fra 1982:

> «Personvern kan være den interesse fysiske og juridiske personer har i å utøve kontroll med den informasjon som beskriver dem.»

I forlengelsen av å se personvern som en interesse i å utøve kontroll med personinformasjon, ble det formulert – i hovedsak i det rettsinformatiske miljøet ved Universitetet i Oslo – en oversikt over forskjellige andre interesser som knytter seg nært opp til interessen i å ha kontroll over egen opplysning.

---

[1] Jf. NOU 1974: 22, *Persondata og personvern* (Sandvik-utvalget); og NOU 1975: 10, *Offentlige persondatasytem og personvern* (Seip-utvalget).

Dette arbeidet resulterte i at personvern ble ansett ikke bare som én interesse, men som et knippe med interesser – en tilnærming som ofte går under navnet «interesseteorien». Den mest innflytelsesrike fremstillingen av denne teorien på 1970- og 80-tallet finnes i Blekeli og Selmer (1977). Her oppstilles en katalog av personverninteresser som primært knytter seg til kontekster der opplysninger om en enkeltperson anvendes av myndigheter og andre som grunnlag for å treffe beslutninger om personen selv.

De sentrale interessene her er beskrevet som *interessen i diskresjon* (dvs. ønsket om å ha kontroll med opplysninger om seg selv, herunder hvilke opplysninger som samles inn av hvem, hvem som har tilgang til disse og hva de brukes til), *interessen i innsyn* (dvs. den enkeltes interesse i å være orientert om hvordan behandling av opplysninger om dem skjer), *interessen i fullstendighet* (dvs. den enkeltes ønske om at avgjørelser som treffes på grunnlag av personopplysninger blir truffet på et fullstendig og korrekt grunnlag) og *interessen i privatlivets fred* (dvs. en generell interesse i å være i fred for andre).

Det er i tillegg oppstilt flere interesser som ikke knytter seg i så stor grad til enkeltindivider, men til kvaliteten på samfunnet generelt. Disse er beskrevet som *interessen i borgervennlig forvaltning* (dvs. at borgernes ønske om at forvaltningen fremstår på en brukervennlig måte), *interessen i vern mot maktmisbruk og overdreven kontroll* (dvs. at overvåkningsnivået i samfunnet skal være begrenset og at kontrollen fra det offentlige ikke er så omfattende at det ikke er rom for et tillitsforhold mellom samfunnet og den enkelte) og *interessen i et robust samfunn* (dvs. et samfunn som i minst mulig grad er sårbart).

Denne interessekatalogen har siden blitt nyansert, omformulert og utvidet av flere forskere og andre eksperter på området. Den mest omfattende fremstilling per i dag finnes i Schartum og Bygrave 2004, se særlig kapittel 2. Interesseteorien (eller kanskje rettere sagt interessemodellen) har et pedagogisk formål, dvs. å forklare innholdet i personvernbegrepet. Den er også et forsøk på å «operasjonalisere» personvern, særlig i sammenhenger der personvern skal veies opp mot andre interesser og hensyn.

4.1.2 Et særnorsk begrep

Betegnelsen «personvern» (uansett definisjon) er langt på vei et særnorsk begrep. I noen få tilfeller er begrepet – eller en nær variant av det – tatt i bruk i andre nordiske land, men kun av enkelte forskere i enkelte publikasjoner, se for eksempel von Koskull (1996) og Blume (1995, s. 17).

I Sverige fokuserer man hovedsakelig på «integritet»; begreper som brukes er blant annet «integritetsskydd» og «personliga integritet». Dette kommer for eksempel til utrykk i den svenske Integritetsskyddskomiteens innstilling fra 2007 (se f.eks. Integritetsskyddskommittén 2007). I Danmark fokuseres det mer på «persondata», «personinformasjon» og beskyttelse av slike, se for eksempel Blume (2003). Begrepet «privatliv» er også benyttet. Peter Blume fokuserer hovedsakelig på begrepet «databeskyttelse» og beskyttelse av det «informationelle privatliv». I følge Blume omfatter sistnevnte vern av det vi kaller privatlivets fred og personlig integritet. Bestemmelser om «databeskyttelse» omfatter derimot regler som sikrer informasjonskvalitet, datakvalitet, systemkvalitet, innsynrett og informasjonsplikter.

4.1.3 Personvernbegrepets røtter

Personvernbegrepet har røtter i eldre begreper som «personlighetsvern» og «personlighetens rettsvern». De eldre begrepene er tradisjonelt blitt brukt som betegnelser på regler som verner visse sider ved den enkeltes personlighet. Formuleringene er noe diffuse og forskjellige, men kretser rundt begrep som «integritet», «menneskeverd» og «sjelelig fred». Bratholm (1968, s. 289) skriver f.eks. at:

> «personlighetsvernet omfatter det vern som den enkelte nyter mot at hans selvrespekt eller menneskeverd krenkes på en utilbørlig måte.»

Selmer (1955, s. 33) skriver at:

> «Rettsvern for personligheten foreligger overalt hvor en person kan påberope seg rettsregler som verner ham mot påvirkninger som erfaringsmessig fører til sjelelig ufred eller overlast.»

Med en litt annerledes dog komplementær fokus skriver *Arnholm* at «personlighetsvern» omfatter:

> «reglene om hvordan den enkelte er sikret mot inngrep i hans ønsker om særliv og samliv innenfor det samfunn han lever i. (Arnholm 1959, s. 83)»

4.1.4 Nyere litteratur og forsøk på avgrensing av begrepet

Selv om det eksisterer klare forbindelser mellom det personvernbegrepet som oppsto på 1970-tallet og disse eldre begrepene, har enkelte forskere hevdet at det også foreligger klare forskjeller i fokus og kontekst. Schartum (1993) skriver eksempelvis:

> «Til tross for slektskap er imidlertid forskjellen forholdsvis stor mellom det tradisjonelle «personlighetens rettsvern» og det moderne personvernet. Personvernteorien og personregisterloven kan langt på vei sies å ha tatt utgangspunkt i edb-teknologi og den datamaskinbaserte saksbehandling som i løpet av 1960-årene ble introdusert i offentlig forvaltning og i store private organisasjoner. Mens en ved å hevde det tradisjonelle «personlighetens rettsvern» forholdt seg til enkelthendelser vedrørende enkeltpersoner, forholder det moderne personvernet seg til systematisk forekommende beslutninger og hendelser vedrørende større deler av befolkningen.»

Bing (1991, s. 33) skriver i samme retning:

> «[P]ersonvern har å gjøre med det moderne informasjonssamfunnets teknologi – ikke med skandalepresse, nærgående fotografer eller dokumentarfilm. Det er først og fremst reaksjonen på automatisk behandling og sammenstilling av store mengder personopplysninger […] som betegnes av dette ordet.»

Disse uttalelsene fra både Schartum og Bing ble skrevet tidlig på 1990-tallet. Begge forskere tilhører det rettsinformatiske miljøet ved Universitetet i Oslo som dyrket fram personvernbegrepet med en intensjon om at begrepet primært (hvis ikke utelukkende) skulle knyttes opp mot moderne former for informasjonsbehandling, særlig «masseforvaltningens» storskalabruk av edb. Siden (i hvert fall) begynnelsen av 1990-tallet har det imidlertid skjedd en markant utvidelse – i hovedsak utenfor dette forskningsmiljøet – i personvernbegrepets bruksområde. Utviklingen skyldes delvis begrepets etymologiske røtter (som omtalt ovenfor) og delvis dets diffuse konturer.

I 1993 anvendte *Den nasjonale forskningsetiske komité for medisin* begrepet som betegnelse på «etiske og rettslige normer som tar sikte på beskyttelse av individet både med hensyn til fysisk og psykisk integritet» (Den nasjonale forskningsetiske komité for medisin 1993, s. 12). *Boe-utvalget* uttalte i NOU 1993:22 at «[p]ersonvern […] i hovedsak [betyr] vern om den personlige integritet». Utvalget la til:

> «I vid forstand kan personvernbegrepet omfatte alt fra fysiske krenkelser til å bli blottstilt i massemedia …»

Også domstoler, byråkrater og en god del jurister har brukt «personvern» i sammenhenger som tidligere ble ansett å omhandle «personlighetsvern» og/eller «personlighetens rettsvern». Eksempelvis henviser Høyesterett til «alminnelige personvernhensyn» i Rt. 1991, s. 616. Til og med Knut Selmer, som var hovedansvarlig for begrepets fødsel, har uttrykt at «personvern» nå brukes til å dekke alt som tidligere ble dekket av «personlighetens rettsvern» (Selmer 1992, s. 181), og at det følgelig:

> «bare er én side av «personvernet» i vid forstand som Datatilsynet har noe med å gjøre, nemlig den som knytter seg til *registrering av personopplysninger i registre, og bruken av slike registre*. (Selmer 1996, s. 41)»

Likeledes noterer Schartum og Bygrave (2004, s. 13) at «personvern» i den allmenne debatten «har nærmest blitt synonymt med beskyttelse av personlig integritet».

En sondring som går mot strømmen i den allmenne bruken av personvernbegrepet finner vi i innstillingen *Ytringsfrihetskommisjonen* (NOU 1997:27), som skiller mellom «personvern» og «privatlivets fred». Kommisjonen skriver:

> «Det er grunn til å understreke den prinsipielt viktige forskjell mellom «privatlivets fred» og «personvern». Beskyttelsen av privatsfæren («privatlivets fred») har en begrunnelse ut over personvernet, en begrunnelse som går på kollektivets eller samfunnets måte å fungere på. Konkret kan det gjelde hensynet til den offentlige samtale. Personvernet går på den annen side først og fremst på beskyttelsen av personen som offentlig person (offentlig omdømme), og nettopp ikke spesielt som privat person. Dette skille er ikke alltid observert som det bør være i diskusjonen om disse tema.»

Denne sondringen har ikke slått igjennom i allmenn diskurs.

Det er ikke slik at «personvern», i motsetning til «privatlivets fred», søker sin begrunnelse i kun «individuelle» (kontra «kollektive») interesser. Personverndiskurs – i alle fall i det rettsinformatiske miljøet ved UiO – har lenge ansett begge typer interesser som del av «personvernet». Dette

betyr ikke at Ytringsfrihetskommisjonens drøftelse av den betydningen som beskyttelse av «privatliv» har for ytringsfrihet og samfunnet mer generelt ikke er nyttig.

4.1.5 Skillet mellom «personvern» og «personopplysningsvern»

Det har i løpet av de siste fire årene vært gjort flere forsøk på å innføre et skille mellom «personvern» og «personopplysningsvern». For eksempel tar Schartum og Bygrave (2004, s. 13ff) utgangspunkt i det faktum at «personvern» nå anses av allmennheten som «nærmest […] synonymt med beskyttelse av personlig integritet». De beskriver videre «personlig integritet» som et overordnet begrep som betegner en tilværelse preget av andres respekt for den enkelte person, hvor bl.a. kontroll over informasjon om en selv er viktig. De fremholder så begrepet «personopplysningsvern» som:

> «en underkategori av personvern som omhandler normer for behandling av personopplysninger med sikte på å verne om personlig integritet, herunder autonomi og privatlivets fred. (Schartum og Bygrave 2004, s. 13ff)»

Stortingets IKT-melding fra 2006 (St.mld. nr. 17 (2006-2007)) tar også opp skillet mellom personvern og personopplysningsvern. Det heter her (side 130 flg):

> «Eit vesentleg element i personvernet er at ein person i utgangspunktet skal kunne avgjere sjølv kva andre skal få vite om hans eller hennar eigne personlege forhold. Vi kan i denne samanhengen snakke om «personopplysningsvern». Det er primært denne dimensjonen som er underlagd omfattande lovregulering som til dømes personopplysningsloven, helseregisterloven, reglar om teieplikt mv.»

Innenfor EU begynner man også å lage et rettslig skille mellom retten til respekt for «privatliv» og/eller «privacy» på den ene siden og retten til «protection of personal data» («data protection») på den andre siden.

Noe tilsvarende skille har så langt ikke vært særlig synlig i norsk personvernrett og dermed heller ikke i avgjørelser fra Datatilsynet, Personvernnemnda eller domstolene. Følgelig er det per i dag vanskelig å legge til grunn at vi har et tilsvarende klart rettslig skille mellom personvern og personopplysningsvern i norsk personvernrett. Det er dermed selvsagt ikke sagt at man i Norge kun har rett til det ene og ikke det andre.

Etter Personvernkommisjonens mening er det på tide å innføre et klarere formelt skille mellom personvern og personopplysningsvern i norsk personvernrett. En slik begrepsdeling er formålstjenlig for å bringe personverndebatten fremover og på høyde med den internasjonale utviklingen.

En deling og derigjennom klargjøring av de to elementene i det norske integritetsvernet kan også være et egnet pedagogisk grep som gjør det enklere å forklare hva som ligger i dem.

Personvernkommisjonen legger følgende definisjon til grunn i denne rapporten:

- Personvern dreier seg om ivaretakelse av personlig integritet; ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse. Eksempel på en personvernbestemmelse er vernet av privatlivets fred i straffeloven § 390.
- Person*opplysning*svern dreier seg om regler og standarder for behandling av personopplysninger som har ivaretakelse av personvern som hovedmål. Reglenes formål er å sikre enkeltindivider oversikt og kontroll over behandling av opplysninger om dem selv. Med visse unntak skal enkeltpersoner ha mulighet til å bestemme hva andre skal få vite om hans/hennes personlige forhold. Det er denne delen av personvernretten som er underlagt den mest omfattende lovregulering i for eksempel personopplysningsloven, helseregisterloven, regler om taushetsplikt og så videre.

Tilfredsstillende personopplysningsvern er ofte en forutsetning for godt personvern og omvendt. Hensynet til det tradisjonelle personvernet (integritetsvernet) tilsier ofte en begrensning i informasjonstilgang. Dermed ser vi at rettighetene henger nært sammen og at de ikke kan debatteres uavhengig av hverandre. I noen situasjoner vil den ene rettigheten likevel stå godt på egne ben. Personopplysningsvernet vil for eksempel ofte være tilstrekkelig til å begrunne innsyn og åpenhet, som en nødvendig forutsetning for at enkeltpersoner skal ha oversikt og kontroll over behandling av personopplysninger som vedgår dem.

4.1.6 Begrepene personvern og rettssikkerhet

Personvern og rettssikkerhet er to grunnleggende komponenter i en rettsstat. Personvern og rettssikkerhet nevnes ofte i sammenheng, tilsynelatende betraktet som synonymer. Ivaretakelse av personvernet er ofte ansette å innebære ivareta-

kelse av rettssikkerheten og omvendt. Men dersom man går nærmere inn i disse begrepene, vil man se at dette ikke alltid stemmer.

Det tradisjonelle personvernet, forstått som respekt for og beskyttelse av integritet og individets ukrenkelighet, vil ofte gå hånd i hånd med kravet til rettssikkerhet. Det motsatte vil imidlertid ofte være tilfellet med personopplysningsvernet. Grunnleggende rettssikkerhetsgarantier som innsynsrett i forvaltningssaker og fri bevisbedømmelse vil ofte innebære behandling og spredning av personlig informasjon som den registrerte ikke kan ha kontroll over. For å sikre borgernes rettssikkerhet vil det derfor ofte være nødvendig å sette personopplysningsvernet helt eller delvis til side.

Rettssikkerhet er gjerne definert som «den alminnelige sikkerheten for liv, eiendom mv. som rettsordenen gir», se for eksempel Gulbransen (1994). Man skiller mellom 1) sikkerhet for angrep på liv og eiendom mv. fra enkeltpersoner (tyver og drapsmenn) og 2) sikkerhet mot overgrep fra statsmakten (vilkårlig fengsling eller konfiskering av eiendom). Det er den siste forståelsen som er sentral her. Typiske og kjente bestanddeler i begrepet «rettssikkerhet» (såkalte rettssikkerhetsgarantier), er at den offentlige makt blir utøvd med hjemmel i lov og at det finnes konstitusjonelle garantier som setter grenser for statens maktbruk, det grunnleggende kravet til forsvarlig saksbehandling i forvaltningen, kravet om forutberegnelighet i lovgivning og forvaltning og regler som skal sikre den enkelte en rettferdig rettergang, for eksempel kontradiksjonsprinsippet[2].

Begrepet «rettssikkerhet» er tradisjonelt knyttet til forholdet mellom enkeltindividet og staten og står sentralt innenfor forvaltningsretten og strafferetten. Det er ikke vanlig å snakke om rettssikkerhet for enkeltindivider i forhold til andre privatpersoners eller aktørers handlinger. Her ser man altså et skille mellom «rettssikkerhet» og «personvern» ettersom sistnevnte (og personopplysningsvern) jo også omfatter private aktørers virksomhet.

Innholdet i begrepet personvern (slik det tradisjonelt har vært forstått i norsk teori) og begrepet rettssikkerhet vil i mange tilfeller overlappe hverandre. Begrepene kan sies å ha samme kjerne: Å beskytte individets integritet mot overgrep. Personvernet avgrenses imidlertid gjerne til å gjelde individets psykiske integritet. Rettssikkerhetsbegrepet gjelder i hovedsak myndighetenes plikt til å hindre at enkeltindividets psykiske eller fysiske integritet blir krenket.

Det kan være hensiktsmessig å skille mellom det privatrettslige området og det strafferettslige området. På det privatrettslige området favner personvernet ofte videre enn rettssikkerhetstankegangen, og vil sikre individet bedre enn rettssikkerhetsgarantiene alene. På det strafferettslige området er det motsatt. Rettssikkerhetsbegrepet favner videre enn personvernet og omfatter for eksempel også prinsippet om bevisumiddelbarhet[3], uskyldspresumpsjonen[4] og muntlighet[5]. Rettssikkerhet gjelder i større grad den fysiske integritet enn det personvernet gjør. På strafferettens område vil kravet til rettssikkerhet ofte ta opp i seg de personvernrettslige garantiene, og i enkelte tilfeller vil man kunne se at rettsikkerhetsgarantier gir et vern som går utover det personvernet ville gitt den enkelte. Personvern og rettssikkerhet vil imidlertid ikke alltid være sammenfallende hensyn på strafferettens område. Utøvelse av prinsippet om fri bevisførsel kan medføre integritetskrenkelser, for eksempel ved at retten tillater opplesing av private dagbøker eller lignende. I slike tilfeller ser man at ivaretakelse av rettssikkerheten fordrer at personvernet settes helt eller delvis til side. I innstillingen til politimetodeutvalget (jf. NOU 2004:6, punkt 6.4) heter det bl.a. følgende:

> «Rettsikkerhet i snever forstand innebærer noe annet enn integritetsvern. Alle har krav på rettssikkerhet i den forstand at det bare kan gripes inn når lovens vilkår er oppfylt. Det gjelder også personer som kan mistenkes å være involvert i alvorlig kriminalitet. Men den som involverer seg i kriminalitet, svekker selv sitt krav på rettssikkerhet i vid forstand, og må derfor finne seg i et inngrep når lovens betingelser er oppfylt. Det sentrale i integritetsvernet blir derfor at inngangskriteriene formuleres slik at metodebruken innrettes mot dem som kan mistenkes for å være involvert i kriminalitet.»

Et skille mellom det privatrettslige og det offentligrettslige kan også være nyttig fremstillingsmessig. Rettssikkerhet kan betegnes som forvaltningens kodeord, og norsk forvaltningsrett innehol-

[2] Prosessrettslig grunnsetning som går ut på at hver av partene skal ha rett til å bli hørt og å bli bekjent med hva den annen part gjør gjeldende.

[3] At parter og vitner skal forklare seg direkte for den dømmende rett og at andre bevis blir ført direkte for denne.

[4] At enhver skal anses uskyldig inntil det motsatte er bevist.

[5] At bevismateriale som skal fremføres for den dømmende rett har en overveiende muntlig form.

der en rekke regler som er ment å ivareta rettssikkerhet. Viktige rettssikkerhetsregler er blant annet forvaltningslovens regler om partenes innsynsrett (jf. §§ 18 og 19), som har sin parallell i personopplysningsloven § 18.

4.2 Det verdimessige grunnlaget for personvern

Personvern og retten til privatliv kan forstås som en rettighet som begrenser offentlige myndigheters mulighet til å registrere og lagre visse former for informasjon om samfunnsmedlemmene. Totalitære regimer misbruker personopplysninger systematisk, men misbruk av personopplysninger kan skje i alle regimer. En overmektig stat, eller utro tjenere i privat og offentlig sektor, kan også misbruke informasjon om individer og grupper i samfunnet. Det er visse opplysninger som vi betrakter som svært private og sensitive, og som kan gjøre oss sårbare for diskriminering og krenkelse dersom de kommer på avveie. Informasjon om seksuell legning, sykdommer eller religion er eksempler på dette. Nettopp derfor er informasjon om slike forhold definert som sensitive opplysninger.

I Norge brukes «personvern» mest som et juridisk begrep. I dette kapittelet ser vi på egenskaper ved personvernet fra et filosofisk og samfunnsvitenskaplige perspektiv. Personvern referer både til vern av personopplysninger, vern av personlig integritet og vern av privatlivets fred. Videre henger oppfatninger om personvern sammen med oppfatninger om frihet, rettferdighet og skillet mellom det offentlige og det private. Personvern og retten til privatliv begrunnes ofte i at individet har en viss råderett over sensitive personopplysninger og derfor skal ha mulighet til å selv bestemme hva andre personer skal vite om ham eller henne. Videre skal individet ha mulighet til å etablere nære og intime relasjoner uten utilbørlig innblanding og innsyn fra andre. Normative analyser av personvern har tradisjonelt fokusert på spørsmålene om hvor vi skal trekke grensen for myndighetenes og andre borgeres legitime innblanding i folks private liv og hva slags informasjon borgere av et samfunn er pliktige å gi til hvem.

Moderne informasjonsteknologi gjør imidlertid at det er grunn til å reise spørsmål om informasjon som ikke nødvendigvis regnes som sensitiv eller privat skal ha et vern. Økende overvåkning og det at vi stadig legger igjen elektroniske spor medfører at det nesten ikke fins grenser for hva slags personlig informasjon som kan registreres og lagres. Dette gir også mulighet til å sammenstille og analysere informasjon på en helt annen måte enn tidligere.

4.2.1 Personvern og personopplysninger

Personopplysningsloven definerer personopplysninger *«som opplysninger og vurderinger som kan knyttes til en enkeltperson»*. Personvern og retten til privatliv handler ikke bare om å beskytte sensitiv og privat informasjon mot offentlig innsyn, men også om retten til å beskytte individets identitet og retten til å være anonym. Personopplysningsvern kan forstås som vern av individers rett til å ha innflytelse på bruk og spredning av informasjon om seg selv.

Kontroll over privat informasjon blir noen ganger fremstilt som et spørsmål om «eiendomsrett» til personopplysninger. Rent intuitivt kan kanskje personopplysninger oppleves som privat eiendom, særlig sensitive personopplysninger, fordi vi har en oppfatning om at vi selv kan avgjøre hvem som skal ha tilgang til dem. Analogien til eiendomsretten er imidlertid problematisk fordi den gir assosiasjoner til en råderett som er mer omfattende enn det som rettslig sett er tilfelle (Schartum og Bygrave 2004, s. 40). Den fungerer for eksempel ikke som et godt utgangspunkt for diskusjon av spørsmålet om når offentlige myndigheter eller andre personer har legitime krav på personopplysninger. Et eiendomsperspektiv på personopplysninger har imidlertid fått ny aktualitet, først og fremst i forhold til bruk av informasjonsteknologi, fordi personopplysninger i større grad har fått økonomisk verdi og kan byttes bort mot varer og tjenester (Schartum og Bygrave 2004, s. 41). Potensielle fordeler med et eiendomsperspektiv er at personer i større grad er garantert utbytte av at personlige data selges på markedet. Det betyr at begge parter får utbytte av salg av personopplysninger. En annen fordel er at det kan begrense kommersielle aktørers bruk av slike data fordi det faktisk vil koste noe å samle inn personopplysninger (Samuelson 2000). Det er uansett vanskelig å anse personopplysninger som privat eiendom fordi det i alle samfunn vil eksistere en rekke legitime grunner til å overprøve eiendomsretten til personlig informasjon. Personvernet må alltid veies opp mot andre interesser og rettigheter, både samfunnets og andre individers.

Kampen mot terror fører for eksempel til at hensynet til personvernet må avveies mot hensy-

net til samfunnets sikkerhet og trygghet. I tillegg lever vi i en velferdsstat som trenger personopplysninger for at vi skal få de tjenestene vi har krav på. Dersom barn skal få trygge oppvekstvilkår og like muligheter, er det for eksempel viktig med rutiner som sørger for at barnefødsler blir registrert og at barns helse og utvikling følges opp. Dette innebærer registrering og lagring av personopplysninger.

Fra et sosialpsykologisk og moralfilosofisk perspektiv legges det noen ganger vekt på at individets kontroll over personopplysninger er en forutsetning for å kunne utvikle meningsfulle sosiale relasjoner til andre mennesker. Individet inngår i en rekke sosiale relasjoner som inneholder forskjellige handlingsmønstre og sosiale forventninger (Rachels 1975, s. 326). James Rachels hevder at privatliv er nødvendig dersom individet skal kunne danne og opprettholde ulike sosiale relasjoner til andre. Personvernet og retten til privatliv er viktig for å beskytte individers mulighet til å opprettholde og utvikle bestemte sosiale relasjoner upåvirket av informasjon gitt i andre kontekster. Med utgangspunkt i et slikt perspektiv kan personvernet forstås som en rettighet som skal sette oss i stand til å differensiere mellom ulike roller, adferdsmønstre og sosiale forventninger. Det er ikke all informasjon om oss selv som vedkommer alle. Opplysninger om helseforhold er definert som en sensitiv personopplyning, men det er nok lettere å fortelle om benbrudd og idrettskader enn om psykiske lidelser. Den vanlige oppfatningen er at graden av selvbestemmelse over personopplysninger øker med graden av intimitet og sensitivitet. Folks opplevelse av hva som er privat og sensitivt vil imidlertid variere mellom kulturer og mellom generasjoner. I vår egen kultur er det for eksempel blitt mer vanlig å bruke media og Internett som arena for eksponering av sensitive opplysninger og detaljer om folks privatliv. Vanlige folk er blitt mer villig til å dele sine livshistorier eller sykdomshistorier med andre via TV, Internett, aviser og ukeblader.

4.2.2 Glimt fra samfunnsforskning om personopplysningers relevans for håndtering av sosiale relasjoner

Forskning om håndtering av sosiale relasjoner handler blant annet om hvordan vi forvalter personopplysninger (se f.eks. Petronio 2000). Relasjonshåndtering analyseres da ut fra spørsmål som: Hvem deler vi hvilke tanker og opplysninger med? Hvem holder vi dem hemmelig overfor? Hvordan svarer vår omverden på de valgene vi tar mellom deling og hemmelighold? Funn fra dette forskningsfeltet viser at, selv om beslutninger om å dele eller skjule personlig informasjon tas individuelt, så gjelder visse kulturelle mønstre. Disse mønstrene er komplekse og i stadig endring. Det er relativt vanlig at man deler mer informasjon med de man føler står en nærmest, men ikke alltid. I blant kan man være mer tilbakeholden overfor de aller nærmeste enn overfor «nære fremmede». Det kan være vanskelig å dele opplysninger med de som står en aller nærest fordi vi er redde for at de kan ta avstand fra oss.

Informasjonsdeling eller hemmelighold er også et spørsmål om tillit: Hvordan har vedkommende håndtert opplysninger eller tanker du har delt med ham eller henne tidligere? Det er videre et spørsmål om hva slags relasjoner de involverte partene har til hverandre. Er hun din lege? Er han din kjæreste? Er barna du snakker med dine barnebarn? Hvor gamle er de? Hva er det relevant, passende, trygt, nødvendig å dele med vedkommende, og hva bør holdes utenfor relasjonen? Det viser seg at spørsmål om hvilke opplysninger og tanker som deles med hvem i forskjellige relasjoner er kulturavhengig. Ethvert samfunn har både vedtatte og uskrevne regler for hvilke tanker og opplysninger som skal deles med hvem. De kulturelle regelmessighetene læres og avlæres, produseres, reproduseres og endres gjennom en dynamisk praksis. I likhet med andre kulturelle normer er disse reglene også stadig i utvikling, ikke minst skjer dette mellom generasjonene.

Det å kunne veksle, mellom en offentlig sfære der vi er synlige for enhver og en intimsfære som vi deler kun med nær familie og utvalgte venner, er en forutsetning ikke bare for demokratiet, men også for ethvert samfunn. Uten en slik veksling, og uten at den enkelte har en viss kontroll over vekslingen, har vi ikke mulighet for å skille mellom nære og fjerne relasjoner.

Selv om oppfatninger om hva som er sensitivt og privat varierer mellom kulturer, er det rimelig å anta at de fleste mennesker har oppfatninger om at det er noe som er privat og sensitivt og at det er visse former for informasjon de vil skjule for mennesker de selv ikke har valgt å ha en relasjon til. Måten personvernet beskyttes juridisk og sosialt vil imidlertid variere fra kultur til kultur.

Spørsmålet om hvor skillet går mellom deling og hemmelighold av personopplysninger kan også forstås som et spørsmål om fysiske grenser mellom privat og offentlig sfære. Sommeren 2003 ble det gjennomført intervjuer i flere europeiske

byer om publikums syn på videoovervåkning (Sætnan et al. 2004, Helten og Fischer 2004). Mange av de intervjuede svarte at ute i det offentlige rommet – i gater, butikker, kjøpesentre – var det helt i orden med videoovervåkning. På slike steder kan vi ikke regne med å ha hemmeligheter uansett. Derimot var videoovervåkning mindre velkomment nær hjemmet og på steder der vi ofte er avkledd, som for eksempel toaletter, omkledningsrom og idrettsgarderober. «Et sted må grensen gå», som en av de intervjuede sa det. Grensen markeres symbolsk og forsterkes fysisk av klær og vegger. Innenfor disse grensene forventer vi å være i fred for uinviterte blikk (se *www.urbaneye.net*).

4.2.3 Personvern og personlig integritet

Personvern som vern om den enkeltes integritet og autonomi representerer på mange måter den klassiske måten å betrakte personvern på. Begrepet autonomi stammer fra gresk, *auto* som betyr uavhengig. Begrepet *nomos* betyr lov. Autonomi oversettes dermed som selvlovgivning. Begrepet referer til individets evne og rett til å ta selvstendige valg på bakgrunn av egne oververbevisninger og rasjonelle overveielser.

Autonomi inngår i vår forestilling om hva det vil si å respektere individets *integritet*.

Begrepet integritet refererer til individets rett til å uttrykke seg som en fullstendig person med egne meninger, oppfatninger og tanker. Respekt for integritet handler om å verne om individets mulighet til å opptre som en selvstendig person med et relativt fast sett av egenskaper og handlingsmønstre. Det forutsetter at individet ikke blir utsatt for vilkårlig press og oppmerksomhet.

I boken *Personvern i informasjonssamfunnet* (2004) skiller Lee Bygrave og Dag Wiese Schartum mellom ulike integritetskategorier: Geografisk integritet, kroppslig integritet, psykisk integritet, kommunikasjonsintegritet og informasjonsintegritet. Disse integritetskategoriene refererer til ulike moralske krav som vi med rette kan stille til hverandre og til offentlige myndigheter. *Geografisk integritet* innebærer respekt for individets rett til privatliv innenfor visse fysiske, eller territoriale grenser for innblandning. Private hjem regnes for eksempel som et område hvor individet kan opptre fritt uten utidig og illegitim innblanding fra andre. Respekt for *kroppslig integritet* stiller krav om beskyttelse mot kroppslige overgrep og uønsket kroppslig oppmerksomhet (Schartum og Bygrave 2004, s. 24). Selve den fysiske krenkelsen av kroppslig integritet, som for eksempel gjennom vold og drap, faller utenfor personopplysningsvernet i streng forstand. Uønsket kroppslig oppmerksomhet, som for eksempel spredning av bilder av seksuell karakter og registrering av andre kroppslige tilstander, faller imidlertid inn under personopplysningsvernet. Slike ting kan krenke kroppslig integritet, men de kan også krenke psykisk integritet. *Psykisk integritet* omhandler respekt for individets følelser, oppfatninger og mulighet for refleksjon. Psykisk terror som skaper dårlig selvbilde og usikkerhet om egne evner og muligheter er et eksempel på krenkelse av psykisk integritet. Det samme gjelder handlinger som forstyrrer individets mulighet til uforstyrret refleksjon, som for eksempel å lese en annens dagbok. Bygrave og Schartum skriver at psykisk integritet delvis kan føres inn under personvernet:

> «For eksempel kan vi se på det å sette noen i psykologiske tvangssituasjoner eller påføre andre følelsesmessige belastninger som et spørsmål om personvern. […] f.eks. tilfeller der enkeltpersoner utsettes for handlinger som skaper usikkerhet om grunnleggende livsforhold. Således kan ekstreme ventetider for asylsøkere betraktes i lys av personvernet (Schartum og Bygrave 2004, s. 25).»

Kommunikasjonsintegritet stiller krav om å respektere individets rett til uforstyrret kommunikasjon med andre. Det å lytte til andres telefonsamtaler, lese andres e-post eller brev faller inn under området for personvernkrenkelse (Schartum og Bygrave 2004, s. 25). For eksempel kan det å overvåke aktivitet som foregår i skolegården kunne krenke skoleelevers kommunikasjonsintegritet fordi skolegården er arena for lek og samtaler. *Informasjonsintegritet* er forstått som vern av personopplysninger. Rettslige spørsmål knyttet til vern av personopplysninger er behandlet i del II om internasjonal og nasjonal personvernrett.

I tillegg til ovennevnte integritetskategorier, kan integritet forstås som *kontekstuell integritet.* Respekt for kontekstuell integritet medfører at man stiller krav om at normer for hva som er relevant informasjon i ulike kontekster skal respekteres. De fleste mennesker har oppfatninger om hvilken informasjon som er relevant eller passende i forskjellige sammenhenger (Nissenbaum 1998). De fleste av oss protesterer ikke på at legen skal ha opplysninger om helsen vår, at banken skal ha kredittopplysninger når vi søker lån, eller

at lærere skal ha relevant informasjon om barna våre. Problemet oppstår dersom vi blir avkrevd informasjon som vi ikke oppfatter som relevant for den aktuelle situasjonen eller relasjonen. Banken kan for eksempel ikke avkreve informasjon om vår religiøse tilhørighet eller seksuelle legning. Ethvert samfunnsmedlem gir fra seg informasjon om seg selv i mange sammenhenger, både til offentlige myndigheter, kommersielle aktører og andre mennesker. Registrering og behandling av personopplysninger regnes som en forutsetning for en velfungerende velferdsstat, men det forutsetter at aktørene kan stole på at aktuell informasjon ikke misbrukes eller brukes til andre formål enn det de har samtykket til. Det å måtte gi fra seg informasjon som ikke er relevant for situasjonen, bli vurdert på feil grunnlag, eller å oppleve at informasjon blir brukt til noe annet enn det som var formålet, kan være en krenkelse av personvernet. En av grunnene til at mange brukerorganisasjoner har protestert mot IPLOS-registeret, som er omtalt i kapittel 16.5.6.3, er at de opplever at den informasjonen de må gi fra seg ikke står i forhold til innholdet i de kommunale tjenestene de søker om å motta. Kontekstuell integritet kan forklare vår moralske indignasjon når vi opplever at vi må gi fra oss mer informasjon enn det som er nødvendig for å realisere formålet.

De ulike integritetskategoriene som er beskrevet her må forstås som analytiske kategorier som i praksis overlapper og griper inn i hverandre. Med utgangspunkt i disse integritetskategoriene kan retten til privatliv begrunnes i det menneskerettslige prinsippet om enhvers rett til lik moralsk respekt. Vi viser ikke hverandre den respekten alle har krav på dersom vi ikke anerkjenner hverandres krav på integritet.

4.2.4 Vern av privatlivets fred

Forestillinger om privatliv forutsetter at det er noe som ikke er privat, og at det da er offentlig. Begrepet privat er avledet av det latinske «privo» som både betyr å frata noe, og være fri eller løsrevet fra noe. Adjektivet «privatus» refererer til det som er særegent for enkeltindividet uavhengig av staten. Fornemmelsen av å være en privatperson er å være en som ikke er en del av det politiske eller offentlige livet (Englehardt 2000, s. 121).

Begrepet offentlig blir brukt på mange måter. Det kan brukes med referanse til de politiske, juridiske og administrative områdene i samfunnslivet. Det brukes også med referanse til den offentlige diskusjonen som foregår i det sivile samfunnet. Filosofen Jürgen Habermas definerer offentlighet som den sfæren der forhold som angår allmenne interesser diskuteres. Disse diskusjonene foregår i fora som media, foreninger, interesseorganisasjoner, frivillige organisasjoner og politiske partier (Habermas 1992). Det private, til forskjell fra det offentlige, har å gjøre med det som ikke angår allmenne interesser og det som ikke trenger å være gjenstand for offentlig undersøkelse og granskning. Spørsmålet hvor grensen mellom det offentlige og det private går, og spørsmål om hva som faktisk angår allmenne interesser, er selv gjenstand for offentlig diskusjon.

Den feministiske bevegelsen har kritisert tradisjonelle skillelinjer mellom offentlig og privat for å implisitt legitimere undertrykking og kontroll som foregår innenfor områder som regnes som private. Kjønnsbasert sosial urettferdighet og moralske krenkelser av kvinner foregår ikke bare i offentlige relasjoner, men i stor grad også i private relasjoner. Deler av kvinnebevegelsen har fremmet kravet: *Det private er politisk.* Dette er krav om at realisering av rettferdighet og likeverd forutsetter at felleskap som tradisjonelt er betraktet som private, det kan være familien eller religiøse felleskap, må gjøres til gjenstand for politiske vurderinger og reguleringer. Kritikere har hevdet at kravet om å politisere det private er et offentligterroristisk prosjekt som vil utslette oss som privatpersoner, og at kritikken heller bør rettes mot tendensen til at vår frihet i stadig større grad innskrenkes av økende byråkratisk makt (Hiley 2006, ss. 82-83). Om hele vår person gjøres til et offentlig anliggende, kan potensielt alle sider ved vår person gjøres til gjenstand for kollektive drøftinger og politiske vurderinger (Holst 2002, s. 127).

Diskusjonen viser imidlertid at personverninteresser alltid må veies mot andre interesser, og at det private ikke kan defineres som en sfære der individet har ubegrenset frihet. Retten til privatliv bør begrunnes som en individuell rettighet, ikke en sfærefrihet. Kravet om at alle mennesker skal tilskrives universell moralsk respekt gjelder på alle områder i samfunnslivet. Det er ikke slik at det eksisterer et område eller en fysisk grense, hvor individer ikke er beskyttet av loven og grunnleggende menneskerettigheter. Som John Rawls sier: «if the so-called private sphere is alleged to be a space exempt from justice, then there is no such thing» (Rawls 1999, s. 598).

Vi ser også en utvikling der det private i stadig større grad preger den offentlige debatten. Det rettes i stadig større grad fokus på politikere og

kjente personers privatliv, følelser og private relasjoner. Politikere benytter seg også i større grad av en retorikk som tilhører privatlivet og den intime sfæren for å få tilslutning. Eksempler på dette ser vi når spørsmålet om hva slags hund den amerikanske presidenten vil gi barna sine presenteres som et offentlig anliggende, eller når politikere åpner hjemmet og privatlivet sitt for pressen. I *The Fall of Public Man,* utgitt i 1974, som på Norsk har fått tittelen *Intimitetstyranniet*, peker sosiologen Richard Sennett på at den politiske retorikken i stadig større grad gjennomsyres av et språk som tilhører intimsfæren og dagliglivet. Sennett knytter den offentlige kulturens forfall til fremveksten av en intimitetsideologi som han mener blir mer og mer fremtredende i vestlige demokratier. Intimitetsideologien kommer til uttrykk i oppfatninger om at sosiale relasjoner og roller blir mer virkelige, autentiske og troverdige jo mer de gjenspeiler den enkelte persons indre psykologiske tilstand. I følge Sennett fører dette til at offentlig diskurs i større grad blir arena for å uttrykke følelser og personlige egenskaper, og mindre grad arena for diskusjon og endring av samfunnsstrukturer og sosiale betingelser som individet er underlagt (Sennettt 1992, s. 8). Dersom det offentlige i alt for stor grad blir et forum for eksponering av privatlivet, vendes oppmerksomheten bort fra saker som angår offentlige interesser. Samfunnsborgerne blir da mer publikum for ulike former for selvpresentasjon enn deltakere i demokratiske prosesser. Privatisering av det offentlige blir også drøftet i kapittel 13 om media og personvern.

4.2.5 Rett til privatliv: Individuell frihet og kollektivt gode

Moderne teorier om retten til privatliv og personvern kan føres tilbake til opplysningsfilosofi, kontraktteori og tidlig liberalisme som utviklet seg fra 1600 tallet. I denne sammenhengen brukes begrepet «liberalisme» som en fellebetegnelse på forskjellige teorier som for det første argumenterer for individets frihet og likeverd, og for det andre er opptatt av å undersøke grensene for legitim statlig maktutøvelse. Begrepet liberalisme brukes imidlertid på mange måter. Det er vanlig å skille mellom det vi kaller politisk liberalisme og økonomisk liberalisme. Politisk liberalisme og sosial liberale teorier understreker verdien av personlig frihet og individets integritet og verdighet. Disse teoriene representerer på mange måter en syntese mellom klassiske argumenterer for individets frihet og sosialdemokratiske argumenter for likeverd og rettferdighet. Økonomisk liberalisme brukes som betegnelse på teorier og ideologier som forsvarer kapitalistisk markedsøkonomi hvor markedet i hovedsak skal styre seg selv uten innblandning fra staten.

Argumenter for personvern bygger i hovedsak på ideer om personlig frihet og individuell verdighet og integritet. Grunntanken er at ethvert individ har rett til et område hvor det kan handle uavhengig av tvang eller innblanding fra staten eller andre samfunnsborgere. Liberal samfunnsteori og politisk teori ble utviklet som en reaksjon på at staten hadde ubegrenset rett til innsyn i alle slags affærer, både personlige og politiske. Det vil si den eneveldige tanken om at individets liv i sin helhet er underlagt fyrstens myndighet. Ideen om rett til privatliv ble også utviklet som en reaksjon på at staten skal oppdra individene til utvikle de «rette» moralske holdninger. I *A Letter Concerning Toleration* (1689) argumenterer John Locke for at spørsmål som angår religiøse overbevisninger er en privatsak som ligger utenfor område for legitim statlig regulering. Tanken om at staten skal være nøytral med hensyn til samfunnsborgernes livssyn, religiøse og kulturelle og familiære verdier har stått sentralt i liberal samfunnsteori. Poenget er at alle har krav på et handlingsrom eller en sfære der man kan utvikle sosiale relasjoner, danne preferanser og ideer uten at myndighetene blander seg inn.

Kritikere mener liberalismen fremmer oppfatninger om at mennesker primært er individualistiske og opptatt av å verne om sine egne interesser fremfor kollektive interesser. De mener videre at liberalismen både forklarer og forvarer en oppfatning om at individet er et uavhengig subjekt som er i stand til å ta selvstendige strategiske valg uavhengig av de normene og verdiene innebygd i det samfunnet, kulturen og de sosiale miljøene han eller hun er en del av (se for eksempel Sandel 1996). Denne kritikken kalles ofte den kommunitaristiske kritikken av liberalismen. Kommunitarisme er en samlebetegnelse på forskjellige normative teorier som undersøker grunnlaget for moral, selvforståelse og frihet i lys av individets sosiale og kulturelle tilknytning og tilhørighet. Kommunitarister mener at dersom frihet primært er forstått som fravær av hindringer og retten til å være alene, så undervurder vi verdien av solidaritet, felleskapsfølelse og samarbeid.

I Two *Concepts of Liberty* (1969) skiller filosofen Isaia Berlin mellom positiv og negativ frihet. Negativ frihet betyr frihet *fra* ytre tvang, og inne-

bærer at alle har rett til et område hvor det kan handle uavhengig av ytre reguleringer, være seg staten eller andre samfunnsborgere. Sentrale negative friheter er ytringsfrihet, religionsfrihet og retten til privatliv. Positiv frihet betyr frihet *til,* og referer til individets frihet til å realisere seg selv som medlem av et samfunn og sosiale felleskap. Det handler med andre ord om personers muligheter til å realisere seg selv som sosiale og politisk aktører, og til å sammen realisere demokrati som et felles prosjekt. Begrepet positiv frihet har røtter i en filosofisk tradisjon som argumenterer for å oppheve skillet mellom private og kollektive interesser, og for at frihet først og fremst handler om å realisere seg selv som en del av staten og samfunnet. Berlin forsvarer negativ frihet og er bekymret for at ideen om positiv frihet kan misbrukes til forsvare paternalisme og totalitære regimer. Forsvarere av negativ frihet er opptatt av at individet skal beskyttes fra statlig kontroll, men også fra konformitetspress og sosial kontroll. I et demokratisk samfunn trenger vi begge formene for frihet. Individet har krav på fravær fra ytre tvang, men demokrati forutsetter imidlertid at individene har mulighet til å utøve innflytelse på de beslutningene som angår dem selv. Dette forutsetter at samfunnsborgere må ha frihet til å delta, det vil si positiv frihet (Lavik og Fjørtoft 2008, s. 172).

Personvern og retten til privatliv faller inn under kategoriene negativ frihet fordi det handler om frihet fra utilbørlig innblanding i personers personlige anliggender. Personvernet er imidlertid også viktig for å beskytte kollektive goder. Valget står ikke mellom frihet til og frihet fra. Personvern og vern av privatlivets fred er en forutsetning for at samfunnsborgere skal kunne realisere seg som aktive deltakere i demokratiske diskusjoner. Retten til privatliv er viktig for å sikre en pluralistisk diskusjon der aktørene er fri til å tematisere forskjellige interesser, behov og synspunkter. Samfunnsdeltakelse forutsetter muligheten til å trekke seg tilbake, gjennomføre selvstendige refleksjoner og til å danne seg oppfatninger på egen hånd. Det forutsetter også at samfunnsborgere kan opptre som offentlige aktører, uten at hele livet deres eller alle trekk ved personen deres blir gjenstand for offentlig diskusjon.

Det å begrense samfunnsborgernes personvern og rett til privatliv kan sette demokratiet i fare. Det at stadig flere offentlige plasser blir kameraovervåket, kan for eksempel resultere i at folk blir redde for å delta på lovlige demonstrasjoner. I verste fall kan registrering og lagring av elektronisk kommunikasjon misbrukes til å hindre eller disiplinere lovlige politiske aksjoner eller sosial uro.

En av de fremste forsvarere av negativ frihet er John Stuart Mill, som i *On Liberty* (Mill [1859] 1991) forsvarer ytringsfriheten. Grunntanken er at ethvert demokrati er avhengig av åpne og opplyste diskusjoner. Demokratisk diskusjon skaper politisk, moralsk og vitenskaplig fremskritt. Opplyst demokratisk diskusjon forutsetter også privatliv. Samfunnsborgere skal ha frihet både fra statlig kontroll, fra sosiale konvensjoner og flertallets meninger, slik at de kan skape sitt eget liv etter sitt eget hode. Mill gir en utilitaristisk begrunnelse for ytringsfriheten og vern om privatlivet. Privatlivet skal beskyttes fordi det er nyttig for samfunnet som helhet og menneskelig trivsel generelt. Utilitarisme er en fellesbetegnelse på teorier som vurderer handlingers moralske verdi mot prinsippet om mest mulig lykke for flest mulig. En rent utilitaristisk begrunnelse av retten til privatliv og personvern kan være problematisk fordi det vil være for lett å ofre enkeltindividers eller gruppers integritet til fordel for økt samfunnsnytte. Man kan for eksempel tenke seg en situasjon der majoriteten kan ha nytte av å begrense svake minoriteters personvern.

På den andre siden skal personvernet veies opp mot samfunnets interesser og andre rettigheter. I den europeiske menneskerettskonvensjonen (EMK) slås det fast at inngrep i utøvelsen av retten til privatliv ikke skal finne sted, med mindre det er i samsvar med loven og nødvendig for nasjonal sikkerhet, for økonomisk velstand, for å forebygge kriminalitet, for å beskytte helse og moral eller beskytte andre rettigheter og friheter. Personvernet må veies opp mot formålet om å forebygge terror og annen kriminalitet, behovet for helse og velferd, retten til innsyn i demokratiske beslutningsprosesser, forskning og andre rettigheter. Det at personvernet er fastslått som en menneskerettighet, innebærer at tiltak som skal øke velferdsnivået eller sikkerheten i et samfunn alltid må vurderes opp mot spørsmålet om hvordan enkeltindividers menneskeverd og autonomi best blir ivaretatt.

Personvern og retten til privatliv beskytter altså rettigheter og friheter som igjen beskytter grunnleggende offentlige friheter, som friheten til å delta i demokratiske prosesser. Det er imidlertid viktig å ikke tenke personvernet primært som instrument for ytringsfrihet og fri offentlig diskusjon. Personvernet bør gis en selvstedig begrunnelse i menneskerettslige prinsipper om verdighet og moralsk respekt.

4.3 Undersøkelser om personvernets stilling

Personvernkommisjonen har ikke hatt mulighet til å gjennomføre selvstendige studier av personvernets stilling i dagens samfunn. I stedet vil vi vise til tre rapporter (Ravlum 2005b, Ravlum 2005a, Bjørnskau et al. 2007) fra Transportøkonomisk Institutt. De to første rapportene presenterer resultater fra spørreundersøkelser som ble utført på oppdrag av Moderniseringsdepartmentet og Datatilsynet av TNS Gallup i mai 2005. Transportøkonomisk Institutt hadde ansvaret for det faglige innholdet av undersøkelsene og for analyse av resultatene. Den tredje er en undersøkelse finansiert av Norges Forskningsråd og tar blant annet for seg hvordan norske beslutningstakere i transportsektoren vurderer forholdet mellom aktuelle sikkerhetstiltak rettet mot terrorisme og kriminalitet, og personvern.

Den første undersøkelsen tar for seg publikums holdninger og praksiser i forhold til personvern. Nedenfor oppsummeres de mest sentrale funnene:

- Fødselsnummer er den personopplysningen de fleste (90 %) mener det er viktig at lovverket beskytter mot innsamling og videre bruk av.
- Andre personopplysninger som 50 % eller flere mener det er viktig å verne er opplysninger om helse (85 %), privat økonomi (80 %), familieforhold (63 %), lokasjonsdata (60 %) og mobiltelefonnummer (50 %).
- Under halvparten mener det er viktig å beskytte flere av de opplysningene som personopplysningsloven definerer som sensitive. Dette gjelder politisk oppfatning (42 %), og religiøs oppfatning (31 %) og fagforeningsmedlemskap (26 %).
- Over halvparten av respondentene sier at de er svært lite eller lite bekymret for at personopplysninger kan bli misbrukt i ulike situasjoner og i forbindelse med ulike handlinger de ble spurt om. Unntaket er bruk av Internett, hvor 61 % sier at de er svært eller noe bekymret for misbruk av personopplysninger.
- 14 % oppgir at de har gitt fra seg personopplysninger i bytte mot en gratis vareprøve eller et godt tilbud. I den yngste aldersgruppa (15-29 år) er dette tallet 27 %.
- 87 % oppgir at de er helt eller delvis enig i at de er forsiktige med å legge igjen personopplysninger på Internett. Likevel svarer et flertall (57 %) at de sjelden avbryter pålogging til Internett, selv om de blir bedt om personopplysninger de ikke ønsker å gi fra seg.
- Over 80 % har ikke benyttet seg av retten til innsyn i hvilke opplysninger som finnes om dem hos offentlige eller private virksomheter. 70 % av disse oppgir at den viktigste grunnen til ikke å benytte innsynsretten enten er at de ikke har reflektert over at det finnes opplysninger om dem eller at de ikke bryr seg om hvilke opplysninger som finnes om dem.
- Hele 58 % sier at personvernet er så godt ivaretatt i Norge at man trygt kan gi fra seg personopplysninger.
- Hele 82 % er helt eller delvis enige i at politiet skal kunne overvåke Internett uten at det foreligger grunn til mistanke. Nærmere halvparten (42 %) er helt eller delvis enig i at helsepersonell kan utveksle helseopplysninger uten samtykke fra pasienten.
- Holdningen til kameraovervåkning er til dels motstridende. Mens 91 % sier seg helt eller delvis enig i at det er greit med kameraovervåkning på offentlige steder, og 79 % svarer at kameraovervåkning får dem til å føle seg tryggere, oppgir 41 % at de ikke liker at stadig flere steder blir kameraovervåket, og hele 50 % er helt eller delvis enig i at kameraovervåkning bare bidrar til å flytte vold og hærverk.
- Nesten samtlige respondenter (97 %) mener det er positivt med kamera i bank- og postlokaler. 81 % mener det er positivt med kamera inne på bussen og toget og i butikker, og 78 % mener det samme om drosjer. Selv blant dem som sier at de ikke liker at stadig flere steder blir kameraovervåket, er det et stort flertall som mener det er positivt med kamera inne på bussen, toget og i drosjer, i bank- og postlokaler og i butikker.
- Respondentene har gjennomgående svært stor tillit til offentlige organers evne til å behandle personopplysninger. Best ut kommer politiet, som 91 % sier de har tillit til, dårligst er sosialkontorene (81 %).
- I privat sektor nyter bankene stor tillit (87 %), mens tilliten er markant lavere til bompengeselskaper (47 %) og teleselskaper (45 %).

Undersøkelsen avdekker at det er gjennomgående stor tillit i befolkningen, både til hvordan ulike offentlige organer og de fleste private virksomheter behandler personopplysninger, og at personvernet i Norge blir ivaretatt på en god måte. Svært få av respondentene uttrykker bekymring for at personopplysninger kan bli misbrukt. Overraskende nok ser dette også ut til å gjelde dem som sier at de *ikke* stoler på at personvernet er så godt ivaretatt at man trygt kan gi fra seg personopplys-

ninger. Mange gir altså tilsynelatende samtykke til innsamling og behandling av personopplysninger selv om de ikke ønsker det.

På bakgrunn av dette mener Ravlum at undersøkelsen viser at samtykke fremstår som særlig problematisk som et tilstrekkelig vilkår for behandling av personopplysninger i en del situasjoner (Ravlum 2005b, s. II).

Den andre rapporten tar for seg behandling av personopplysninger, holdninger til personvern, samt kunnskap om personopplysningsloven og oppfølging av de plikter som følger av den hos 424 norske virksomheter. Også dette er en ren spørreundersøkelse, slik at resultatet baserer seg på de svar virksomhetene har gitt. Forskerne har ikke undersøkt om svarene som er gitt gir et riktig bilde av virkeligheten.

Undersøkelsen viser at det finnes en grunnleggende positiv holdning til personvern blant virksomhetene.

Kunnskapen om personopplysningsloven og de krav den stiller er imidlertid lav. Svært mange av virksomhetene mener at kravene ikke gjelder for dem, selv om de behandler personopplysninger og følgelig er omfattet av loven.

Hele 30 % av virksomhetene oppgir at de ikke har oppfylt noen av kravene som følger av personopplysningsloven eller forskriften. Bare 4 % oppgir at de har oppfylt samtlige krav (etablert internkontrollsystem, definert behandlingsansvarlige, skaffet oversikt over hva slags personopplysninger som behandles, gjennomført risikovurdering, gitt informasjon til den som opplysningene gjelder, etablert rutiner for sletting av opplysninger som ikke lengre er nødvendige i forhold til formålet).

Den tredje rapporten var en kvalitativ undersøkelse med dybdeintervjuer som tok for seg hvordan norske beslutningstakere i transportsektoren vurderer forholdet mellom aktuelle sikkerhetstiltak rettet mot terrorisme og kriminalitet, og personvern. Det generelle inntrykket er at personvern ikke er gjenstand for stor oppmerksomhet i norske transportvirksomheter, men at de ulike aktørene har vurdert personvernimplikasjonene av tiltak i egen virksomhet. Ingen av respondentene mente at avveiningen mellom sikkerhet og personvern var et stort problem.

4.4 Overvåkning og kontroll

I hovedverket *Democracy in America* (Tocqueville [1835] 2003) poengterer den franske samfunnsviteren Alexis de Tocqueville at et moderne demokrati innebærer et velferdssamfunn som i sin tur forutsetter byråkratisk dokumentasjon og intervensjon. Eksistensen og tilgjengeligheten av velferdsgoder skaper en risiko for at godene misbrukes. Som et mottrekk introduserer samfunnet teknologier for overvåkning og kontroll. Disse teknologiene skal forsøke å forhindre at godene blir misbrukt, sørge for at de fordeles rettferdig, og at de tilflyter riktig person. «Klassiske» eksempler på slike teknologier er: Folkeregisteret, identitetspapirer, selvangivelse og bokettersyn.

Michel Foucault hevder i boka *Surveiller et punir*[6], at mange av modernitetens manifestasjoner (skoler, sykehus, fengsler, fabrikker og storbyer) har oppstått gjennom ringvirkningene av ulike overvåknings- og kontrollteknologier. Overvåkning og kontroll er således ifølge Foucault både en forutsetning for, og en konsekvens av, det moderne samfunnet.

I introduksjonen til sin bok om overvåkningssamfunnet (*Surveillance Society*) skriver den kanadiske sosiologen og overvåkningseksperten David Lyon (2001) at det engelske ordet for «overvåkning» (*surveillance*) opprinnelig er et fransk ord som direkte oversatt betyr å «våke over» eller «passe på». Dette uttrykket, fortsetter Lyon, rommer den ambivalens at det både kan være et uttrykk for *omsorg* og for *kontroll*. I dagligtalen kan man be noen om å «passe på» et barn. Meningen kan være å forhindre at barnet roter seg bort i trafikken og blir overkjørt, eller å kontrollere at barnet ikke gjør ugagn. Den samme dobbeltbetydningen finner vi for øvrig i det norske ordet «overvåke».

Datatilsynets direktør, Georg Apenes, gir uttrykk for en tilsvarende ambivalens når han hevder at «storebror» (utlagt som den totalitære og kontrollerende stat i George Orwells *1984*), går hånd i hånd med «store mor» – et omsorgsvesen som ifølge Apenes representerer «velferdsstatens overideologi» (Apenes 2008).

I tradisjonell sosiologisk litteratur brukes «overvåkning» gjerne om systematisk og rutinemessig innsamling og behandling av personopplysninger med det formål å utøve innflytelse, administrasjon, styring og kontroll (se for eksempel Lyon 2001, s. 2).

I sin moderne form handler overvåkning om å finne, lagre, og bearbeide faktiske opplysninger knyttet til enkeltindivider. Fordi praktisk talt all

[6] Bokstavelig oversatt: «Overvåk og straff», men på norsk har den fått den noe misvisende tittelen *Det moderne fengsels historie* (Foucault 1977).

innsamling, lagring, søking, gjenfinning, og analyse av opplysninger er tuftet på bruk av informasjonsteknologi, handler overvåkning i vår tid i stadig økende grad om bruk av slik teknologi.

Akkurat hva slags personopplysninger som samles inn og bearbeides gjennom overvåkningsaktiviteter varierer, men inkluderer blant annet tekstytringer, lydopptak, videoopptak, biometriske spor som fingeravtrykk og DNA, lokasjonsdata, trafikkdata og data som avdekker sosiale relasjoner.

Tradisjonelt har overvåkning vært utført av staten, som en del av politimessig og etterretningsmessig arbeide for å sikre nasjonen mot indre og ytre fiender. Den brede tilgangen på informasjonsteknologi som kjennetegner vår tid har imidlertid endret dette, slik at teknologi for overvåkning også er tilgjengelig for kommersielle aktører, organisasjoner og privatpersoner.

Som vi skal se i kapittel 14.4 er det krefter som er pådrivere for å øke den statlige teknologisk baserte overvåkningen, gjerne begrunnet med «sikkerhet» eller «krigen mot terror». Men også den private overvåkningen øker. Her er motivene kommersielle. Overvåkning av forbrukeratferd gir blant annet overvåkeren mulighet til å produsere individuelt tilpasset reklame, noe som gir høyere salg gjennom økt kontroll over den enkelte forbruker.

Kommisjonen har ikke klart å finne data som gir entydige svar på hvorvidt ulike former for overvåkning fungerer kriminalitetsforebyggende eller om overvåkning bidrar til at flere forbrytelser blir oppklart. Samtidig ser det ut til at privat videoovervåkning av kommersielle rom (som kjøpesentre og liknende) virker sosialt ekskluderende. Enkeltindivider som etter visse kriterier betraktes som «uønsket» identifiseres vha. overvåkningskameraene, slik at en vekter kan sendes ut for vise vedkommende bort fra området (Lomell 2007).

Når det gjelder den overvåkningen av forbrukeradferd som utføres av en del tjenesteytere på Internett, ser den ut til å ha den effekt at de ledende selskapene på dette området også nyter stor kommersiell suksess.

4.4.1 Echelon, FRA-loven og EUs datalagringsdirektiv

Takket være det kjølvannet av biologiske og elektroniske spor som vi gjennom bruk av moderne kommunikasjonsteknologi hele tiden etterlater oss, er det mulig for de som måtte ha interesse av dette å få tilgang på langt mer data om hver enkelt av oss og våre bevegelser, enn noen gang tidligere. Eksempler på dette ser vi blant annet i det USA-dominerte Echelon-systemet, den svenske FRA-loven og EUs datalagringsdirektiv.

Echelon er et svært omfattende system for avlytting av elektronisk kommunikasjon. Det omfatter telefontrafikk, e-post-meldinger, faksmeldinger, tekstmeldinger og internettbruk. Formelt drives systemet i fellesskap av USA, Storbritannia, Canada, Australia og New Zealand, men i praksis domineres systemet av USA og NSA (National Security Agency). Echelon har vært operativt siden 1970-tallet og ifølge Bye og Sjue (2008, s. 493) brukes systemet til industrispionasje, politisk spionasje og spionasje mot diverse organisasjoner.

USA benekter at systemet eksisterer, men det er beskrevet i flere detaljerte bøker (Bamford 2002; Hager 1996; Lyon 2001) og EU-rapporter. Europaparlamentets *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)* konkluderer med at systemet eksisterer.

Den svenske såkalte «FRA-loven» gir det statlige organet Försvarets Radioanstalt (FRA) fra 1. januar 2009 adgang til å overvåke all kabelbåret teletrafikk som krysser Sveriges grenser.

Beskrivelser av systemet som FRA-sjefen Ingar Åkesson har gitt i diverse intervjuer, tilsier at overvåkningen omfatter e-post, websider, telnet (protokoll for virtuell terminal), ftp (File Transfer Protocol, filoverføring over Internett), tekstmeldinger, chat, samt fast- og mobiltelefonsamtaler.

Rent praktisk skjer overvåkningen ved at systemet kontinuerlig og automatisk analyserer data som passerer teleoperatørenes knutepunkter og identifiserer etterretningsmessig interessant informasjon. Når en melding eller samtale flagges som «interessant», kopieres denne fra teleoperatørens knutepunkt til FRA for nærmere analyse.

Akkurat hva som skal til for at en melding eller samtale skal betraktes som «interessant», er en hemmelighet. Men antagelig er det snakk om avanserte algoritmer som ser på mange ulike faktorer, som for eksempel bestemte stemmeavtrykk, bestemte avsendere og mottagere, og selvsagt forekomster av ulike kombinasjoner av ord, som «attentat» eller «atombombe».

Mens FRA-loven hjemler overvåkning og analyse av innholdet i elektronisk kommunikasjon, tar EUs datalagringsdirektiv (direktiv 2006/24/EF av 15. mars 2006) sikte på å sikre politiet tilgang til såkalte «trafikkdata» ved å pålegge teletilbyderne å lagre disse dataene i en viss tid (mini-

mum 6, maksimalt 24 måneder), slik at de kan utleveres til politiet dersom politiet trenger dem til sin etterforsking i dette tidsvinduet.

Innholdet i kommunikasjonen skal ikke lagres, men direktivet krever at tilbydere av kommunikasjonstjenester (dvs. teleselskaper, mobiloperatører, bredbåndsleverandører) skal lagre:

- Data som er nødvendige for å spore og identifisere kilden til en kommunikasjon, enten det dreier seg om fasttelefoni, mobiltelefoni, internettadgang, e-post eller IP-telefoni.
- Data som er nødvendige for å spore og identifisere termineringspunktet for en kommunikasjon, enten det dreier seg om fasttelefoni, mobiltelefoni, e-post eller IP-telefoni.
- Dato, klokkeslett for inn- og utloggingstidspunkt, IP-adresse, bruker-ID, DSL-linje og abonnentidentifikasjon for internettadgang.
- Dato, klokkeslett og samtalevarighet, og abonnentidentifikasjon, telefonlinje for mobil og fasttelefon
- Lokasjonsdata som viser hvor mobilt utstyr befant seg da en samtale ble koblet opp.

4.4.1.1 Grenseoverskridende overvåkning

Det som kjennetegner mange moderne systemer for overvåkning, er at de ikke bare er grenseoverskridende i bokstavelig forstand (dvs. de er systemer som, i likhet med den kommunikasjon de retter seg mot, er globale og grenseoverskridende). De er *kvantitativt* sett så omfattende at de også passerer en *kvalitativ* grense ved å etablere overvåkningsregimer som overskrider en grense for hva som er forholdsmessig og bikker over til å bli en systematisk og gjennomgripende registrering av et stort antall opplysninger som i utgangspunktet ikke er knyttet til bekjempelse av kriminalitet og terrorisme. I stedet registreres svært mye data tuftet på den antagelse at noe av det som registreres kanskje en gang i fremtiden kan vise seg å komme til anvendelse.

Erfaringen viser også at når data først er registrert, vil det ofte være vanskelig å hindre at de blir brukt til nye formål. Dette kalles for «funksjonsutglidning» eller «formålsutglidning», (engelsk: *function creep*) og beskrives av Fox (2001, s. 261) som:

> «Previously authorised arrangements […] are now being applied to purposes and targets beyond those envisaged at the time of installation»

Et svært dramatisk eksempel på formålsutglidning er når bostedsstatistikk som ble samlet inn av Statistisk Sentralbyrå for rene statistikkformål før krigen ble benyttet av okkupasjonsmakten under krigen for å lokalisere norske jøder som ble sendt til Tyskland for utslettelse (Hannemyr 2005, s. 107). Erfaring, inklusive nevnte eksempel fra vår egen historie, viser at data som er lagret gjerne blir brukt til andre formål enn de som er tiltenkt. Det gir grunn til å utvise stor varsomhet ved lagring av data.

Ut fra erfaringen med at DNA-identifisering framstår som et forløsende bevis i enkelte alvorlige saker, har land etter land utvidet sin innhenting, lagring og bruk av DNA-spor. Dette fører ikke bare til at flere saker oppklares, men også til at en økende del av befolkningen står, varig, i nasjonale DNA-registre. Dette resulterer ikke bare i økt oppklaring av saker, men også i endringer i borgeres rettigheter. Blant annet er det en konsekvens av å stå i et DNA-register at man til enhver tid står i en virtuell identifiseringskonfrontasjon (engelsk: *line-up*). Mens det ellers er en frivillig sak å delta i identifiseringskonfrontasjoner, er dette ikke lengre frivillig for den som står i et DNA-register. DNA-identifiseringsteknologien muliggjør videre at denne identifiseringskonfrontasjonen også omfatter de registrertes slektninger. Williams og Johnson (2004) skriver om denne trinnvise utvidelsen av DNA-søkingen at det dannes hele sjikt av samfunnet som havner under konstant overvåkning.

Dahl og Sætnan (2008) påpeker at formålsutglidning gjerne kan skje med de aller beste hensikter, uten at resultatet av den grunn blir akseptabelt.

Kommisjonen vil i særdeleshet bemerke at tiltak av den type som det legges opp til i EUs datalagringsdirektiv setter både personvernet og ytringsfriheten på prøve. Dette vil gjelde selv om lagring av trafikkdata i henhold til direktivet ikke anses som kontinuerlig eller regelmessig overvåkning av borgerne. Verdien av lagring må også veies opp mot effekter på frimodighet. Dette gjelder selv om formelle friheter ikke berøres, og selv om de registrerte data kun skal være tilgjengelige for politiet under regulerte forhold. Bare visheten om at noen kan lete seg fram til dine kontakter og dine bevegelser, både i det fysiske rommet og på Internett, kan være nok til å hemme borgere i utøvelsen av sine friheter til å samles, til å ytre seg og til å søke opplysninger. Dette er grunnleggende rettigheter i et demokrati, som kommer til uttrykk både i norsk lovgivning og i Den europeiske menneskerettskonvensjon (EMK). Etter kommisjonens oppfatning vil innføring av direktivet kun-

ne svekke opplevelsen av privatliv og privat kommunikasjon.

EMK artikkel 8 annet ledd åpner riktig nok for at samfunnet kan gjøre inngrep i personvernet. Men for at et slikt inngrep skal være forsvarlig, må det blant annet være *nødvendig i et demokratisk samfunn.* I dette ligger det etter Den Europeiske Menneskerettighetsdomstolens (EMD) praksis at det må være en «pressing social need» for å gripe inn i personvernet. Det holder ikke at det er hensiktsmessig, rimelig eller ønskelig. Inngrepet som gjøres må dessuten være proporsjonalt i forhold til formålet som ønskes oppnådd.

Både den overvåkningen av innholdet i elektronisk kommunikasjon som gjøres av Echelon, som planlegges innført i Sverige, og den omfattende lagringsplikten av trafikkdata som følger av EUs data lagringsdirektiv, er etter Personvernkommisjonens oppfatning problematisk i forhold til nødvendighetsprinsippet og proporsjonalitetsprinsippet.

4.4.2 Kommersielle selskapers overvåkning av sine brukere

Mange av de mest dominerende kommersielle selskapene som tilbyr sluttbrukere gratis tjenester på Internett benytter en forretningsmodell der kundene bytter tjenester mot personopplysninger. Google og Facebook er eksempler på slike selskaper.

Ofte er hjemmelsgrunnlaget for disse selskapenes behandling av personopplysninger samtykke fra brukeren. I noen tilfeller er samtykket underforstått. På en plakat på selskapets hjemmeside står det at gjennom å bruke tjenesten godtar man automatisk at personopplysninger samles inn og behandles. Et slikt underforstått samtykke tilfredstiller ikke lovens krav til et frivillig, uttrykkelig og informert samtykke.

Andre selskaper opererer med et mer aktivt samtykke. Gjerne i form av en tilsvarende plakat som vises fram før brukeren får tilgang på tjenesten, der brukeren eksplisitt må tilkjennegi at han eller hun samtykker ved å «klikke» på en knapp på skjermen (såkalt *Clickwrap*) Mange av disse plakatene er imidlertid utformet på måter som er svært vanskelige å forstå, med språklige grep som snarere villeder enn veileder. For at samtykke skal være gyldig behandlingsgrunnlag i Norge, må det ikke bare være eksplisitt, det må også være «informert» (dvs. forstått av den som samtykker). Er samtykket ikke informert, er det heller ikke gyldig.

4.4.3 Økonomisk regulering av personvernulemper

De vanligste måtene å styrke personvernet på er enten juridisk (gjennom lover og forskrifter), og didaktisk (gjennom informasjon og opplæring). Personvernkommisjonen ønsker imidlertid å vise til at man også på enkelte områder bør overveie økonomiske virkemidler.

I et økonomisk perspektiv kan man betrakte personvern som et gode det er knapphet på (og som det, etter kommisjonens mening, mest sannsynlig vil bli mindre av). Ved å sette en *kostnad* på et tiltak som kan ha negativ effekt for personvernet, kan det bidra til at det gjøres en kritisk vurdering hos tiltakshaver om hvorvidt de positive effektene han vil oppnå (sikkerhet, dokumentasjonsbehov, etc) er så store eller viktige at de oppveier den kostnaden han vil måtte betale (i form av en avgift som representerer ulempen som tiltaket vil ha i forhold til personvernet).

I et slikt økonomisk perspektiv vil en kostnad i form av en avgift føre til at de dårligst begrunnede tiltakene vil falle bort, rett og slett fordi antatt nytte ikke anses å oppveie kostnaden. Personvern er da ikke lenger bare et mykt hensyn som man kan velge å ta hensyn til, men også en pris som må betales.

I praksis vil en slik tankegang bare kunne brukes på noen få personvernområder. Et som peker seg ut som et eksempel, er kameraovervåkning av offentlig rom. (Dette bør defineres klart, men grovt regnet menes det steder der allmennheten har fri tilgang). Det offentlige rom er et sted der vi alle har en forventning om å kunne ferdes fritt.

4.4.3.1 Organisasjon, innkreving og inntekt

Et avgiftssystem vil kreve en organisasjon for oversikt og innkreving. Når det gjelder oversikten, kan vi se til Sverige der tillatelse til overvåkning av offentlig rom gis av länsstyrelsen og er regulert i en egen lov. Annen kameraovervåkning reguleres av den svenske personuppgiftslagen. Tilsvarende er det i Norge foreslått at kommunene kan gi tillatelser/skal holde oversikt over kameraovervåkning. Fordelen med en slik delegering er at den skaper en lokal arena for diskusjon om hvilke overvåkningstiltak vi aksepterer – og hvilke vi ikke vil ha.

Dagens meldeskjema for kameraovervåkning ber ikke om informasjon om antall kameraer som plasseres ut. Derfor finnes det ifølge Datatilsynet ingen oversikt over hvor mange kameraer som i

dag overvåker offentlige rom i Norge. Vi må kunne gå ut fra at det er mange tusen. Kommisjonen gjetter på at en årlig avgift på noen få tusen kroner pr. kamera vil være tilstrekkelig til at behovet for å overvåke det offentlige rom tenkes gjennom på nytt. På grunn av det store antall kameraer, vil selv en beskjeden avgift likevel gi en betydelig inntekt, som f.eks. kan brukes til å styrke Datatilsynet, eller til å styrke personvernet på annet vis.

4.5 Fra data til personopplysninger

4.5.1 Data og informasjon

Ordet *data* er egentlig flertallsformen av den latiniske termen «datum», som betyr «noe som er gitt». I dagligtalen brukes ordet data i første rekke om faktiske opplysninger eller kjensgjerninger. Ordet kan imidlertid også vise til andre former for ytringer, som erfaringer, meninger, instruksjoner, kunngjøringer og liknende. I dagligtalen er det ikke noe klart skille mellom data og det beslektede begrepet *informasjon*.

I forbindelse med *elektronisk databehandling* (EDB) skiller man imidlertid mellom «data» og «informasjon».

I EDB-diskurs brukes «data» spesifikt om den *fysiske representasjonen* av kjensgjerninger, etc. Representasjonen kan være i form av tekst (skrift på papir), eller i form av fysiske tilstander i en maskin (eksempel: lyd-, lys- eller elektriske signaler).

I et moderne EDB-system representeres imidlertid alltid data signaler, der hvert signal bare kan befinne seg i en av to mulige tilstander (dvs. tilstanden er binær). Et enkeltstående binært signal kalles for et «bit» (sammentrekning av de to engelske ordene «*bi*nary» og «digi*t*». Et bit er altså den *minste* dataenheten. For å representere mer komplekse data (for eksempel bokstaven «A») setter man sammen flere bit. I de fleste EDB-systemer benyttes 8 bit til å representere ett enkelt tegn i det latinske alfabetet. For bokstaven «A» benyttes for eksempel bitsekvensen «01000001». Ved å sette sammen tilstrekkelig mange bit til en datamengde kan man representere data av vilkårlig kompleksitet. Personvernkommisjonens delrapport om personvern og media (50 sider med tekst) består av litt over 2 milliarder bit. Rådata for et enkelt bilde fra et moderne digitalkamera med 10 millioner bildelementer (megapiksler) utgjør typisk 120 millioner bit.

I EDB-diskurs brukes ordet «informasjon» som betegnelse for det *meningsbærende innholdet* som lar seg trekke ut når «data» fortolkes og forstås. Mens data i første rekke behandles maskinelt og overføres mekanisk, kreves det et tenkende menneske for å forstå hva slags *informasjon* en bestemt datamengde representerer.

Som et eksempel som belyser forskjellen på data og informasjon, kan vi ta for oss kontosystemet i en bank. I et slikt EDB-system vil bankkundenes navn, adresse og fødselsnummer være representert i form av *data* i systemet, sammen med innestående på konto og alle pengetransaksjoner inn på og ut av konto. Når slike data trekkes ut og presenteres på en meningsfylt måte, for eksempel i form av de kontoutskriftene som hver måned blir sendt til kundene, er det tale om *informasjon*.

4.5.2 Opplysninger

Ordet *opplysninger* har ikke noen spesiell betydning i forhold til EDB, og brukes gjerne om både data og informasjon.

Som vi ser i neste avsnitt står imidlertid begrepet *personopplysning* i en særstilling i forhold til personopplysningsloven. Så langt Personvernkommisjonen forstår, bruker personopplysningsloven begrepet «opplysning» der en EDB-tekniker ville brukt ordet «data» – altså om kjensgjerninger om personer som er gitt en fysisk representasjon. Men opplysningsbegrepet i loven omfatter også meningsinnholdet – det vil si informasjon – som kan utledes fra dataene, se for eksempel Schartum og Bygrave (2004), avsnitt 4.3.3. Som utdypet i neste avsnitt, kommer personopplysningsloven først til anvendelse når dette meningsinnholdet kan knyttes til en enkeltperson.

På engelsk brukes for øvrig uttrykket «personal data» om det som heter «personopplysninger» på norsk.

4.5.3 Personopplysninger

En avklaring og avgrensning av begrepet «personopplysning» er viktig for forståelsen av personopplysningslovens virkeområde. I dette avsnittet redegjør Personvernkommisjonen for den forståelsen av begrepet som legges til grunn videre i rapporten.

Personopplysningslovens formålsparagraf (§ 1) er nært knyttet opp til bruk og behandling av personopplysninger:

> «Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av *personopplysninger*. Loven skal bidra til at *personopplysninger* blir behandlet i samsvar med grunnleggende personvern-

hensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på *personopplysninger*. (vår uthevning)»

Vurderingen av om en opplysningstype faller inn under lovens definisjon av personopplysninger er derfor avgjørende for om loven kommer til anvendelse eller ikke.

Begrepet personopplysninger er definert i personopplysningsloven § 2 nr. 1 som:

«Opplysninger og vurderinger som kan knyttes til en enkeltperson.»

En tilsvarende definisjon er lagt til grunn i EUs direktiv om personopplysningsvern (Direktiv 95/46/EF) artikkel 2 a):

"'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

Dette utgangspunktet må nyanseres noe, og dette kan best gjøres ved å dele definisjonen opp i fire elementer. Definisjonen omfatter 1) enhver form for informasjon som 2) kan knyttes til 3) en identifisert eller identifiserbar 4) fysisk person. Nedenfor vil vi kort gå gjennom de ulike elementene av definisjonen. De fire elementene henger nært sammen med hverandre, og det enkelte element står ikke uten de tre andre. Av metodiske hensyn blir de likevel behandlet separat i det følgende.

Lovgiver har lagt til grunn en svært vid tolkning av begrepet, i tråd med direktivet. Hensikten var å omfatte all informasjon som kan knyttes til et individ, med en så generell definisjon som mulig. Det er samtidig viktig å få til en god balanse i definisjonen av begrepet. Begrepet må ikke favne for vidt, slik at personvernregler kommer til anvendelse på forhold hvor det ikke er nødvendig. Samtidig må ikke begrepet tolkes for snevert, slik at viktige behandlingsformer faller utenfor. For å oppnå denne balansen er det viktig å legge opp til fleksibilitet i lovverket.

Artikkel 29 gruppen i EU[7] har i Opinion 4/2007 (Art 29 WP 2007) uttalt seg om begrepet «personopplysninger». Sammen med forarbeidene til personopplysningsloven og annen relevant nasjonal praksis, legges denne uttalelsen til grunn for gjennomgåelsen som følger.

4.5.3.1 Enhver form for informasjon

Valget av betegnelsen «enhver form for informasjon», viser lovgivers intensjon om en vid forståelse av hva som skal anses som en personopplysning. At lovgiver legger opp til en vid tolkning følger også av forarbeidene, se for eksempel NOU 1997:19, punkt 10.1.1 og kapittel 21 og Ot.prp. nr. 92 (1998-1999), punkt 4.2.2 og kapittel 16.

Definisjonen omfatter altså enhver form for informasjon – både opplysninger og vurderinger. Med *opplysninger* forstår man faktabaserte former for data knyttet til en person, som for eksempel navn, adresse og alder. Med *vurderinger* forstås mer sammensatte former for data, som ofte vil være basert på én eller flere opplysninger. Opplysningsformer som faller inn under denne kategorien vil være informasjon om at «NN er en solid kunde» eller «NN er en vanskelig pasient og må behandles nennsomt». Det er ikke nødvendig at opplysningene er sanne eller bevist på noen måte.

Andre former for opplysninger som vil kunne omfattes av lovens definisjon er opptak av telefonsamtaler, for eksempel hvor en kunde gir instruksjon til bank eller tradingdesk. Bilder fra kameraer og videoovervåkning vil også kunne være informasjon som omfattes av lovens definisjon, såfremt de kan gi opplysninger om en enkeltperson, se nedenfor.

Når det gjelder innholdet av informasjonen, omfattes både sensitive opplysningsformer så vel som mer generelle former for informasjon. Begrepet «personopplysning» omfatter både opplysninger som stammer fra individets privatliv og familieliv, samt informasjon som stammer fra andre aktiviteter individet utfører, for eksempel i arbeidslivet og gjennom økonomiske eller sosiale relasjoner.

En særskilt informasjonsform er biometriske data. Biometriske data kan defineres som biologiske egenskaper og psykologiske karakteristikker som er unike og målbare. Typiske eksempler på slike biometriske data er fingeravtrykk, mønsteret på netthinnen og iris, ansiktsform og stemme. Slike former for data vil som hovedregel være personopplysninger.

Humant biologisk materiale, som for eksempel hår, hud eller genprøver, vil i utgangspunktet ikke være personopplysninger, da de ikke gir utrykk for opplysninger om en bestemt person i seg selv. Sli-

[7] Artikkel 29-gruppen er et rådgivende organ i saker om personvern i EU, og består av representanter fra alle medlemslandenes datatilsyn. Det norske Datatilsynet er også representert, men har formelt sett kun status som observatør.

ke former for data skal altså ikke som sådan behandles som personopplysninger etter loven. Dette har blant annet blitt slått fast av Personvernnemnda i klagesak 2002/8. Informasjon som kan utledes av biologisk materiale vil imidlertid kunne være personinformasjon og dermed falle inn under definisjonen av begrepet personopplysning. Forutsetningen er at informasjonen som kan utledes av dataene kan knyttes til en bestemt person. Tilknytningskriteriet behandles under neste punkt.

4.5.3.2 Tilknytningskriteriet

Vi har nå slått fast at definisjonen som gis i direktivet og personopplysningsloven i utgangspunktet er svært vid med hensyn til hvilke former for data som kan omfattes. Det neste elementet i definisjonen oppstiller imidlertid et kriterium om at dataene må kunne knyttes til en fysisk person. Dette elementet av definisjonen er svært viktig, ettersom det er her man knytter det som i utgangspunktet kun er ulike former for data til et enkelt individ. Det blir derfor avgjørende å finne hvilke relasjoner mellom data og individ som er relevante.

På et generelt nivå kan man si at en opplysning knytter seg til et individ når opplysningen *handler om* individet.

Artikkel 29 gruppen har uttalt følgende om dette:

> "data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated (Art 29 WP 2005a, s. 8) og (Art 29 WP 2007)."

Tilknytningen kan være både direkte og indirekte. Opplysninger som vil være *direkte* knyttet til individet, er for eksempel opplysninger om navn og personnummer. En mer *indirekte* tilknytning får man der opplysninger *kan* knyttes til personen, for eksempel opplysninger om telefonnummer, bostedsadresse, bilregistreringsnummer eller yrkestittel. Ved slike indirekte koblinger mellom data og individ må gjerne flere opplysninger undersøkes før persontilknytningen kan bringes på det rene. Det er altså ikke noen vilkår for at loven skal komme til anvendelse at en på et gitt tidspunkt vet hvilken person det foreligger opplysninger om – at det er mulig å identifisere vedkommende er nok.

I mange situasjoner er det lett å fastslå en slik tilknytning mellom opplysning og individ. Dersom opplysningene er lagret i en personalmappe er de klart knyttet til et enkeltindivid (den ansatte). Det samme gjelder dersom opplysningene er lagret i en pasients epikrise eller når personen er filmet under et videointervju.

Det er imidlertid mange situasjoner hvor det ikke er like enkelt å fastslå om data er knyttet til et individ eller ikke. Dette vil typisk være situasjoner hvor dataene direkte knytter seg til *fysiske objekter*, som for eksempel et telefonnummer, en IP-adresse eller bilregistreringsnummer. Dataene refererer altså ikke opprinnelig til et fysisk individ, men til et objekt (telefon, datamaskin eller bil). Spørsmålet er om slike former for data skal regnes som personopplysninger eller ikke. Svaret beror på om det lar seg oppstille en kobling mellom objektet og en eier. Objektene som dataene relaterer seg til eies som regel av noen, slik at man indirekte kan knytte dataene til et fysisk individ. Et bilregistreringsnummer kan gjennom offentlige registre spores tilbake til hvem som er registrert som eier av bilen. Et bilregistreringsnummer vil derfor som hovedregel være å regne som en personopplysning. Tilsvarende vil gjelde for en servicelogg på en bil som ligger hos forhandler. Opplysningene kan relateres enten til eier eller til mekanikeren som jobbet på bilen og vil derfor være personopplysninger. Også verdien av et hus kan i visse tilfeller være en personopplysning. Dersom opplysningen om husets verdi kun benyttes for å illustrere eiendomsprisene i et gitt distrikt, vil det ikke være en personopplysning, såfremt huset ikke er individuelt identifisert i denne konteksten. Men huset vil samtidig være noens eiendom, og opplysninger om huset knytter seg dermed indirekte til eierens plikt til å betale skatt. I slike situasjoner vil opplysninger om husets verdi også være å betrakte som en personopplysning.

Eksemplene viser at det vil foreligge en «personopplysning» selv om det er flere ledd mellom opplysningene og individet og selv om man må undersøke flere steder for å etablere koblingen mellom opplysning og individ. Det må imidlertid trekkes en skjønnsmessig grense med hensyn til hvor stor innsats som kreves for å knytte data til et individ. Dersom det kreves stor arbeidsinnsats og/eller kostnad å knytte dataene til et individ, kan dette tale for at en ikke anser opplysningen for å være «personopplysning».[8] Tilsvarende må man ta forbehold dersom det er usikkerhet med

---

[8] Se fortalen (nr. 26) i Direktivet om personopplysningsvern hvor det heter «*to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person*. ». [Vår uthevning.] Dette elementet i definisjonen er ikke så tydelig i den norske loven og fremkommer heller ikke av forarbeidene. Det er imidlertid klart at en tilsvarende reservasjon må innfortolkes i den norske loven.

hensyn til tilknytningen mellom dataene og individet. Situasjonen kan for eksempel være at det er flere personer som er brukere av samme maskinidentitet på Internett (IP-nummer), og maskinen ikke er registrert som eiet av en bestemt fysisk person. Usikkerheten med hensyn til hvilken person opplysningene gjelder, vil da kunne tale for å ikke anse kravet om tilknytning til en enkeltperson for å være oppfylt.

4.5.3.3 Et identifisert eller identifiserbart individ

Det neste elementet man må se på i definisjonen er om dataene kan sies å være relatert til et identifisert eller identifiserbart individ. Kravet om identifisering følger klart av personverndirektivets artikkel 2 (a):«*'personal data' shall mean any information relating to an identified or identifiable natural person*».

Kriteriet fremgår ikke klart av den norske lovteksten, men det følger av forarbeidene at tilsvarende må oppstilles også etter norsk lov:«*Med 'personopplysning' menes opplysninger og vurderinger som direkte eller indirekte kan knyttes til en identifiserbar, fysisk person (den registrerte)*», (se NOU 1997:19 kapittel 21, merknader til lovens § 2).

Det oppstilles altså et identifikasjonskrav, og for at en opplysning skal regnes som en personopplysning etter loven, må opplysningen eller vurderingen kunne knyttes til en bestemt person.

Generelt kan man si at en person er identifisert når han eller hun er «skilt ut» fra en større eller mindre gruppe. Følgelig vil en person være «identifiserbar» når det er mulig å skille vedkommende fra andre individer, selv om det ennå ikke er gjennomført noen slik identifikasjon.

Et individ kan identifiseres ved utvendige kjennetegn, som for eksempel utseende, høyde, vekt, hårfarge eller bekledning. Videre kan det identifiseres gjennom kvaliteter som det innehar, som for eksempel yrke, funksjon eller navn. Identifikasjonen kan skje direkte, for eksempel ved individets navn, eller indirekte gjennom for eksempel telefonnummer eller en sammensetning av ulike data som gjør det mulig å snevre inn og peke ut det konkrete individet opplysningene relaterer seg til.

Muligheten for identifikasjon vil imidlertid være situasjonsbetinget. Et alminnelig familienavn som «Hansen» vil ikke være tilstrekkelig for å identifisere en person i en større forsamling. Men i en skoleklasse eller på en arbeidsplass kan det være tilstrekkelig å kjenne familienavnet for å knytte data til det konkrete individet som bærer navnet Hansen.

I mange situasjoner må man også sammenholde ulike former for data for å sikre at man har identifisert rette person. Navnet «Hansen» sammenholdt med fødselsdato, opphav, adresse og bilde vil gjøre det mulig å identifisere én bestemt person ved navn Hansen i en gruppe hvor flere bærer dette navnet.

Individer kan også identifiseres indirekte gjennom unike kombinasjoner av data, i større eller mindre utstrekning. For eksempel vil opplysninger om «politimesteren på Stryn» alene være en identifiserbar personopplysning. I andre tilfeller må man sammenholde flere former for data, for eksempel «Oslo-advokat», alder, inntekt og type firma, for å kunne identifisere en konkret person. Det samme gjelder fragmentariske opplysninger i pressen. Ofte ser man at pressen ikke publiserer navn eller andre direkte identifiserende former for data, men samtidig publiserer data som gjør at man lett kan få tilgang til ytterligere informasjon, og dermed oppnå identifikasjon.[9]

Også under dette elementet av definisjonen er det imidlertid nødvendig å sette en begrensning med hensyn til hvor omfattende tiltak som skal til før man oppnår sikker identifisering. En hypotetisk mulighet for identifisering er ikke nok til at man kan si at dataene er identifiserbare. Dersom det ikke er mulig eller kun ubetydelig sannsynlighet for at man oppnår identifisering, skal man ikke anse individet for «identifiserbart». Følgelig vil ikke dataene være å regne som «personopplysninger» etter loven. Momenter som er relevante i denne vurderingen er ressursbruk og kostnadene ved å gjennomføre en eventuell identifisering, formålet brukeren har med behandling av dataene, hvordan behandlingen er lagt opp og fordelene og ulempene ved en eventuell identifisering for både brukeren (den behandlingsansvarlige) og den som identifiseres. Hvilken teknologi som er tilgjengelig i dataenes «levetid» er også et moment. Dersom dataene skal lagres i en måned og teknologien i dag ikke tilsier at dataene vil bli relatert til en identifisert person, så taler det for at dataene ikke blir regnet som personopplysninger. Motsatt dersom dataene skal lagres i 10 år og man må

[9] Et eksempel på dette er den såkalte «Lommemann-saken» våren 2008. Ingen aviser offentliggjorde navnet på mannen eller bildet av ham, men ved å gi informasjon om kjønn, alder, bosted, inntekt og formue, yrkesmessig status og hobby var det svært enkelt å finne ut hvem mannen var. Han ble altså identifisert gjennom fragmenter av data som ble satt sammen slik at det ga en positiv identifikasjon av vedkommende.

anta at den teknologiske utviklingen gjør identifisering sannsynlig.

Også opplysninger som fremstår som anonymiserte kan være «personopplysninger», såfremt det finnes referanser eller andre tilknytningspunkter som gjør identifisering mulig. Et eksempel som nevnes i forarbeidene er en internettbasert tjenesteleverandør som registrerer en anonym elektronisk identitet som bare kan knyttes til en identifiserbar enkeltperson dersom man har tilgang til opplysninger som vedkommendes internettleverandør sitter inne med (se NOU 1997:19, kapittel 21, merknader til § 2). Slike elektroniske spor vil være å regne som personopplysninger, selv om man trenger opplysninger fra tredjepart for å knytte dataene til en identifiserbar person. Det samme vil gjelde for pseudonymiserte og krypterte former for data, ettersom noen vil sitte på en nøkkel som gjør opplysningene lesbare og dermed vil kunne identifisere personen som opplysningene gjelder. Dette vil gjelde selv om tilknytningen mellom personen og opplysningen bare er kjent av noen få personer. Der man står overfor opplysninger som er anonymisert på en slik måte at det ikke lenger er mulig å knytte dataene til en identifiserbar enkeltperson, er det ikke lenger snakk om «personopplysninger». Det er likevel viktig å være klar over at dataene teknisk sett kan være anonymisert, men likevel knytte seg til en så liten gruppe at tilhørigheten røpes på en mer indirekte måte som er belastende for den opplysningen gjelder. Man vil da stå overfor data som må betegnes som «personopplysninger», ettersom identifisering likevel er mulig indirekte (se Ot.prp. nr. 92 (1998-1999), s. 101).

4.5.3.4 Fysisk person

Det fjerde og siste elementet i definisjonen er at dataene må kunne relatere seg til en fysisk person. Begrepet eller konseptet «person» regnes for å oppstå ved fødselen og avsluttes ved død. Personopplysninger er dermed i utgangspunktet data som kan relatere seg til levende individer.

Med dette utgangspunktet vil ikke opplysninger om juridiske personer (selskaper, stiftelser, foreninger mv.) være å regne som «personopplysninger» og dermed omfattes ikke slike data av personopplysningsloven.[10]

Når det gjelder opplysninger om døde personer, vil slike data normalt ikke være å regne som «personopplysninger». Unntak oppstilles imidlertid der opplysninger om døde også gir informasjon om levende personer. Opplysninger om at en avdød person led av en arvelig sykdom, vil også gi informasjon om vedkommendes barn. Slike opplysninger vil derfor regnes som «personopplysninger» og være omfattet av loven.

---

[10] Dette i motsetning til den gamle personregisterloven fra 1978, hvor opplysninger om juridiske personer var gitt uttrykkelig vern. Unntak oppstilles imidlertid også etter den nye personopplysningsloven dersom det behandles opplysninger om enkeltmannsforetak eller mindre familiebedrifter, hvor opplysningene om foretaket/bedriften kan ansees som opplysninger om én bestemt fysisk person (eieren). Personopplysningsloven gjelder videre for behandling av kreditt-opplysninger om juridiske personer (jf. § 3 og personopplysningsforskriften § 4-1 (2)).

Del II
Personvernrett – hovedtrekk og hovedutfordringer

Kapittel 5
Innledning

Personvernkommisjonens arbeid har vært knyttet til de utfordringene personvernet møter i dagens samfunn. Gjennom mandatet ble kommisjonen oppfordret til å skildre dagens situasjon og utfordringer for personvernet innenfor ulike sektorer og se hen til internasjonale avtaler og regelverk om personvern.

Det er altså personvernretten som har stått i fokus i kommisjonens arbeid og som har vært vårt rettslige utgangspunkt. Det har imidlertid vært tydelig for kommisjonen at personvern ikke er noen absolutt rettighet, og at denne retten ofte må vike for andre berettigede interesser, som for eksempel ytringsfrihet og kriminalitetsbekjempelse. Det har derfor vært nødvendig for kommisjonen å se hen til lovgivning som skal ivareta andre hensyn og som tangerer eller utfordrer personvernet.

Personvernretten er preget av omfattende regulering, både nasjonalt og internasjonalt.

Denne delen av rapporten presenterer hovedtrekk ved det rettslige regelverket som har personvern og/eller personopplysningsvern som hovedformål. Den beskriver også noen sentrale utfordringer ved anvendelse og utvikling av dette regelverket. Presentasjonen er av overordnet karakter, og fokuset er rettet mot lovgivning som har hatt særlig relevans for kommisjonens arbeid. I tillegg vil personvernbestemmelser og sentrale juridiske problemstillinger innenfor de særskilte områdene kommisjonen har arbeidet med bli gjennomgått i rapportens del IV.

Kapittel 6
Internasjonale regler

Regelverk om personvern og personopplysningsvern som er vedtatt på et internasjonalt eller overnasjonalt plan har vokst enormt de siste fire tiår. Det samme kan sies om dets påvirkningskraft. Enkeltnasjoner (inklusive Norge) får mindre frihet til selv å bestemme hvordan de utvikler nasjonal personvernrett. Det internasjonale regelverket nedfeller et stort antall minstekrav som enkeltnasjoner er forpliktet til å overholde ved utforming av deres egen lovgivning.

Det er imidlertid betydelig variasjon innenfor det internasjonale regelverket med hensyn til reglenes detaljeringsgrad, anvendelsesområde og rettslig status. Deler av regelverket har form av grunntraktater om menneskerettigheter som er nedfelt i kortfattete, svært generelle bestemmelser. Disse traktatene utgjør det sentrale normative grunnlaget for mesteparten av det øvrige regelverket på feltet, både nasjonalt og internasjonalt. Deler av dette øvrige regelverket har form av relativt detaljerte og omfattende regelsett som inneholder en rekke spesifikke krav til behandling av personopplysninger. De viktigste av disse regelsettene er EUs direktiv om personopplysningsvern (direktiv 95/46/EF) og Europarådets konvensjon om personopplysningsvern av 1981. Andre deler av regelverket er derimot i form av «soft law»-instrumenter, dvs. anbefalinger, retningslinjer mv. som formelt sett ikke er rettslig bindende. Disse kan likevel ha stor politisk tyngde og dermed betydelig påvirkningskraft. Det mest innflytelsesrike av disse instrumentene er retningslinjer for beskyttelse og utveksling av personopplysninger over landegrenser som ble vedtatt av OECD (Organisation for Economic Co-operation and Development) i 1980.

De aller fleste av de regelsett som er nevnt ovenfor er utformet på en teknologinøytral og generell måte, slik at de kommer til anvendelse på mange samfunnssektorer og i mange forskjellige teknologiske sammenhenger. I tillegg finnes det et stort antall regelsett som fokuserer på nærmere angitte områder og/eller teknologier – som forskning, telekommunikasjon, biometri og kryptografi. De fleste av disse regelsettene er i form av anbefalinger, retningslinjer eller liknende. Europarådet har vært særlig aktivt med å utarbeide sektorspesifikke anbefalinger. Men det finnes også sektorspesifikke regelsett som er rettslig bindende. EUs direktiv om elektronisk kommunikasjon og personvern (direktiv 2002/58/EF) er et viktig eksempel her.

I det følgende gir vi en kort presentasjon av de mest sentrale instrumentene som utgjør det internasjonale regelverket om personvern og personopplysningsvern. For en mer utførlig gjennomgang, se Bygrave 2008 samt Schartum og Bygrave 2004 kapittel 3.

6.1 Personvern etter menneskerettighetstraktater

De aller fleste traktater om menneskerettigheter inneholder bestemmelser som anerkjenner personvern som grunnleggende rettighet. Dette kommer først og fremst til uttrykk i bestemmelser om retten til privatliv («privacy» eller «private life»). Slike bestemmelser finner vi bl.a. i konvensjoner vedtatt av De Forente Nasjoner (FN) og Europarådet. Bestemmelsene bygger på FNs Verdenserklæring om menneskerettighetene av 1948 artikkel 12 som lyder som følger:

> «Ingen må utsettes for vilkårlig innblanding i privatliv, familie, hjem og korrespondanse, eller for angrep på ære og anseelse. Enhver har rett til lovens beskyttelse mot slik innblanding eller slike angrep.»

6.1.1 FN-konvensjonen om sivile og politiske rettigheter av 1966

FN-konvensjonen om sivile og politiske rettigheter (forkortet «SP») ble vedtatt 16. desember 1966 og trådte i kraft 23. mars 1976. Den inneholder en bestemmelse (artikkel 17) som lyder omtrent det samme som artikkel 12 i Verdenserklæringen:

1. «Ingen må utsettes for vilkårlige eller ulovlige inngrep i privat- eller familieliv, hjem eller kor-

respondanse, eller ulovlige inngrep på ære eller omdømme.
2. Enhver har rett til lovens beskyttelse mot slike inngrep eller angrep. »

FNs Menneskerettighetskomité har uttalt i General Comment nr. 16 av 23. mars 1988 at SP artikkel 17 krever at personopplysninger innen både offentlig og privat sektor blir behandlet i samsvar med grunnleggende prinsipper for personopplysningsvern.

6.1.2 FN-konvensjonen om barns rettigheter av 1989

Konvensjonen om barns rettigheter ble vedtatt den 20. november 1989 og trådte i kraft den 8. januar 1991. Den inneholder en bestemmelse (artikkel 16) med tilnærmet samme formulering som SP artikkel 17, men i forhold til barn:

1. «Intet barn skal utsettes for vilkårlig eller ulovlig innblanding i hans eller hennes privatliv, familie, hjem eller korrespondanse og heller ikke for ulovlige angrep mot hans eller hennes ære eller omdømme.
2. Barnet har rett til lovens beskyttelse mot slik innblanding eller slike angrep.»

6.1.3 Den europeiske menneskerettskonvensjon av 1950

Den europeiske menneskerettskonvensjonen av 1950 (forkortet «EMK») ble vedtatt den 4. november 1950 og trådte i kraft den 3. september 1953. Artikkel 8 lyder som følger:

1. «Enhver har rett til respekt for sitt privat- og familieliv, sitt hjem og sin korrespondanse.
2. Offentlig myndighet skal ikke gjøre noe inngrep i utøvelsen av denne rett med mindre dette inngrep er i samsvar med loven og i et demokratisk samfunn er en nødvendig forholdsregel for den nasjonale eller offentlige sikkerhet, for landets økonomiske velstand, for å forebygge uorden eller forbrytelser, beskytte helse eller moral eller beskytte andres rett og friheter. »

Bestemmelsen pålegger en stat å ha lover som verner privatlivets fred og som verner den enkelte mot å få sin integritet og ære krenket – både av offentlige myndigheter og private aktører. Plikten omfatter også at det må finnes lover som regulerer innsamling, forvaltning og spredning av personopplysninger (jf. videre Schartum og Bygrave 2004, ss. 96-97).

Etter bestemmelsens annet ledd kan imidlertid inngrep i rettighetene som er nedfelt i første ledd være lovlige dersom følgende kumulative kriterier er oppfylt:

(i) Det foreligger et rettslig grunnlag for inngrepet som tilfredsstiller vanlige prosessuelle rettssikkerhetskrav (klarhet, forutberegnelighet mv.);

(ii) Inngrepet er nødvendig, det vil si at det foreligger et påtrengende samfunnsmessig behov («pressing social need») for inngrepet, og inngrepet er forholdsmessig i forhold til det formålet som søkes oppnådd («proportionate to legitimate aim pursued»);

(iii) Inngrepet tjener ett eller flere av formålene som er angitt i annet ledd.

Den europeiske menneskerettighetsdomstolen (EMD) har gradvis erkjent at EMK artikkel 8 rommer et person*opplysning*svern, både i forhold til offentlig sektor og privat sektor. Sentrale avgjørelser i så måte er *Klass mot Tyskland* (dom 1978-09-06), *Malone mot Storbritannia* (dom 1984-08-02), *Leander mot Sverige* (dom 1987-03-26), *Gaskin mot Storbritannia* (dom 1989-07-07), *Niemietz mot Tyskland* (dom 1992-12-16), *Amann mot Sveits* (dom 2000-02-16), *Peck mot Storbritannia* (dom 2003-01-28), *von Hannover mot Tyskland* (dom 2004-06-24), og *Copland mot Storbritannia* (dom 2007-04-03).

I forhold til personopplysningsvernet har EMDs praksis så langt ikke utviklet nye grunnleggende prinsipper utover de som finnes i andre sentrale regelsett på området. Men praksisen legges til grunn ved tolking av andre europeiske regelsett som for eksempel EUs direktiv om personopplysningsvern. Og den betoner krav til klar lovhjemmel og proporsjonalitet/forholdsmessighet ved behandling av personopplysninger, slik at disse kravene også er blitt mer vektlagt og synliggjort ved anvendelse av direktivet og øvrige regelsett på feltet.

Personvernkommisjonen vil fremheve følgende hovedtrekk fra EMDs avgjørelser som særlig viktige for kommisjonens mandat og arbeid. For det første har EMD definert privatliv («private life») relativt bredt. Domstolen fastslår at begrepet omfatter visse aktiviteter som utføres i den offentlige sfære (jf. eksempelvis sakene *Niemietz* og *Peck*). For det andre vil registrering og videre behandling av personopplysninger, uten at den registrerte har gitt sitt samtykke til eller fått kunnskap om behandlingen, i seg selv være et inngrep etter artikkel 8(1) (jf. eksempelvis *Leander* saken). For det tredje, når domstolen vurderer hvor-

vidt en handling utgjør et inngrep i privatliv mv., legges det bl.a. vekt på folks rimelige forventninger om hva som er privat. Et fjerde moment er at registrering og lagring av personopplysninger – uten at disse brukes videre – i seg selv kan være nok til å utgjøre et inngrep i henhold til artikkel 8(1) (jf. *Amann* saken). Det siste momentet er at også private aktørers behandling av personopplysninger kan rammes av EMK artikkel 8 (jf. *von Hannover* saken). Alle disse trekkene er utdypet og drøftet senere i rapporten.

6.1.4 EUs charter om grunnleggende rettigheter av 2000

EUs charter om grunnleggende rettigheter (*Charter of Fundamental Rights of the European Union* (2000/C 364/01)) av 2000 inneholder to bestemmelser med særskilt relevans for personvern og personopplysningsvern. Den første er artikkel 7, som lyder:

> «Everyone has the right to respect for his or her private and family life, home and communications.»

Den andre er artikkel 8, som direkte angår personopplysningsvern. Bestemmelsen består av tre ledd:

1. «Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.»

Charteret er i seg selv ikke rettslig bindende, men det utgjør likevel et viktig utgangspunkt for utvikling av regulatorisk politikk innenfor EU. Det som er særlig verdt å merke seg ved charteret er at det anviser en særskilt rett til «protection of personal data» som del av de grunnleggende menneskerettighetene i EU. Personopplysningsvern er med andre ord blitt ansett som en grunnleggende rettighet i seg selv. Dette synet kommer også til uttrykk i det (hittil mislykkede) forsøket på å få på plass en ny grunnleggende rettslige plattform for hele EU-systemet. I den forbindelse, se eksempelvis traktaten av 2004 om innføring av en europeisk grunnlov (*Treaty establishing a Constitution for Europe*; ikke i kraft) artikler I-51 og II-68 (sml. artikkel II-67) som også oppstiller personopplysningsvern som separat rettighet i forhold til retten til privatliv mv.

6.2 Internasjonale regelsett som direkte angår personvern

6.2.1 Europarådets konvensjon av 1981

Europarådets konvensjon om personvern i forbindelse med elektronisk behandling av personopplysninger (*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* – heretter «Europarådets konvensjon om personopplysningsvern») ble vedtatt den 28. januar 1981 og trådte i kraft den 1. oktober 1985. Den er den eneste konvensjonen som direkte omhandler personopplysningsvern. Konvensjonen er blitt ratifisert av de aller fleste land som er medlemmer av Europarådet, deriblant Norge som ratifiserte den 20. februar 1984. Konvensjonen kan også ratifiseres av land som ikke er medlem av Europarådet (jf. artikkel 23), men denne muligheten er hittil ikke blitt benyttet. Endringer i konvensjonen ble vedtatt i 1999, for at også EU som sådan skal kunne ratifisere konvensjonen, men disse er ennå ikke trådt i kraft.

Ved ratifikasjon forplikter en stat seg til å inkorporere konvensjonens prinsipper i sitt nasjonale regelverk (jf. artikkel 4(1)). Konvensjonen inneholder ellers ikke rettigheter som direkte kan anvendes av enkeltindivider. Den etablerer heller ikke et eget håndhevelsesorgan.

Hovedformålet med konvensjonen er å sikre personvernet mot trusler ved elektronisk databehandling (jf. artikkel 1). Den nedfeller et sett med prinsipper som fastsetter minstestandarder for all elektronisk behandling av personopplysninger (jf. artikkel 5 flg.). Prinsippene gjelder i utgangspunktet kun elektronisk eller automatisert behandling, men kan utvides til også å omfatte manuelle prosesser.

Konvensjonen har samtidig som formål å redusere personvernrelaterte hindre mot overføring av personopplysninger mellom land, for gjennom dette å fremme friheten til å kommunisere og motta informasjon, samt fremme internasjonal handel og økonomisk vekst. Begrunnelsen for dette er at enkelte stater (deriblant Norge) fra før hadde lovgivning om personopplysningsvern som begrenset overføring av personopplysninger til andre land, med mindre opplysningene kunne nyte et vern lik det i opprinnelseslandet (jf. eksempelvis Norges gamle personregisterlov § 36,

samt dens hovedforskrift § 8-1). Konvensjonen fastsetter vilkår for innføring av slike begrensninger, først og fremst i forbindelse med overføring av personopplysninger mellom stater som har ratifisert konvensjonen (jf. artikkel 12). Hovedregelen er at en stat som har sluttet seg til konvensjonen ikke skal hindre overføring av personopplysninger til en annen stat som tilbyr «equivalent protection» for disse opplysningene. Ved en protokoll vedtatt 23. mai 2001 ble konvensjonen tilføyd bestemmelser om overføring av personopplysninger til stater som ikke har ratifisert konvensjonen. Disse bestemmelsene dupliserer langt på vei tilsvarende bestemmelser i EUs generelle direktiv om personopplysningsvern (se videre avsnitt 6.2.4). Protokollen tilføyer videre konvensjonens bestemmelser om nasjonale datatilsynsmyndigheters kompetanse. Også disse bestemmelsene dupliserer i stor grad tilsvarende bestemmelser i EUs direktiv.

I tillegg til denne konvensjonen har Europarådet vedtatt en lang rekke anbefalinger som utdyper reglene i konvensjonen innenfor nærmere avgrensede områder, så som telekommunikasjon, politiarbeid, forskning og statistikk, forsikring og arbeidsliv. Selv om disse anbefalingene ikke er folkerettslig bindende, danner de et viktig utgangspunkt for utarbeidelse og reform av nasjonalt regelverk. De danner dessuten et viktig utgangspunkt for nasjonale datatilsynsmyndigheters praksis.

6.2.2 OECDs retningslinjer av 1980

OECD vedtok den 23. september 1980 retningslinjer for beskyttelse og utveksling av personopplysninger over landegrenser (*Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*). Retningslinjene er ikke rettslig bindende, men har hatt stor innflytelse på utviklingen av nasjonalt regelverk, særlig i ikke-europeiske OECD medlemsland, som eksempelvis Canada, Australia og New Zealand. De har også dannet hovedutgangspunktet for utarbeidelse i 2004/05 av en «Privacy Framework» i regi av Asia Pacific Economic Cooperation (APEC). Sistnevnte instrument nedfeller retningslinjer som skal veilede APEC medlemsland i utforming av deres nasjonale politikk på feltet.

Formålet ved og innholdet i OECDs retningslinjer er langt på vei det samme som for Europarådets konvensjon om personopplysningsvern. Oppnåelse av formålet om å fremme internasjonal handel og økonomisk vekst ved å lette flyt av personopplysninger mellom land var likevel en viktigere drivkraft bak retningslinjene enn det var ved utarbeidelsen av konvensjonen. Likevel er prinsippene for overføring av personopplysninger mellom land og for innsamling og videre behandling av personopplysninger ellers, stort sett like i begge instrumenter.

Med utgangspunkt i retningslinjene fra 1980 har OECD utarbeidet flere andre retningslinjer som berører personopplysningsvern. Disse gjelder bl.a. informasjonssikkerhet (jf. *Guidelines for the Security of Information Systems* (1992); senere erstattet av *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002)), kryptopolitikk (jf. *Guidelines for Cryptography Policy* (1997)), og forbrukervern i forbindelse med elektronisk handel (jf. *Guidelines for Consumer Protection in the Context of Electronic Commerce* (1999)).

6.2.3 FNs retningslinjer av 1990

FNs generalforsamling vedtok den 14. desember 1990 retningslinjer for elektroniske personregistre (*Guidelines Concerning Computerized Personal Data Files*). Retningslinjene inneholder prinsipper for behandling av personopplysninger som stort sett er lik de som finnes i OECDs retningslinjer av 1980 og Europarådets konvensjon av 1981, men utfyller likevel disse på enkelte punkter (se videre Bygrave 2002, s. 73 og 350). Retningslinjene oppfordrer dessuten internasjonale organisasjoner – i tillegg til FN-medlemstater – til å behandle personopplysninger på personvernvennlig vis. Retningslinjene er ikke folkerettslig bindende og synes å ha hatt liten praktisk betydning sammenlignet med øvrige internasjonale regelsett på feltet. De signaliserer imidlertid at interesse for personopplysningsvern i prinsippet rekker utover den vestlige demokratiske sfæren.

6.2.4 EUs direktiv 95/46

EU vedtok den 24. oktober 1995 et direktiv om personopplysningsvern (direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger). Direktivet ble den 25. juni 1999 tatt inn i avtalen om det europeiske økonomiske samarbeid av 1992 («EØS-avtalen»), og ble dermed gjort folkerettslig bindende for Norge. Direktivet utgjør en sentral premissleverandør for norsk regulatorisk politikk på feltet, ikke bare på grunn av EØS-avtalen, men også for-

di direktivet er betydelig mer detaljert og omfattende enn øvrige internasjonale regelsett som for eksempel Europarådets konvensjon av 1981 og OECDs retningslinjer av 1980. Direktivet er gjennomført i Norge i hovedsak ved personopplysningsloven.

6.2.4.1 Formål

I likhet med de to sistnevnte regelsettene, har direktivet to hovedformål: På den ene siden å fremme personvernet, på den andre siden å fremme internasjonal handel ved å avskaffe unødvendige hindre mot at personopplysninger skal kunne overføres mellom land. I henhold til direktivet er det siste formålet i hovedsak relatert til EUs grunnleggende ønske om å realisere målsettinger vedrørende de «fire friheter» ved det indre markedet. Dette kommer bl.a. til syne ved at direktivet forbyr EU/EØS-medlemsland å hindre flyt av personopplysninger til andre medlemsland når hindringen begrunnes med henvisning til personvern (jf. artikkel 1(2)). Selv om direktivets innhold og målsetting er sterkt preget av et ønske om å sikre fri flyt av personopplysninger mellom medlemsland, har direktivet et idealistisk formål om å sørge for et høyt nivå på personopplysningsvern innenfor EU/EØS-området. Dette formålet er siden blitt fremhevet av EF-domstolen (jf. avgjørelse 2003-05-20 i sak C-465/00, *Rechnungshof mot Österreichischer Rundfunk m.fl.* og forente saker C-138/01 og C-139/01, *Neukomm og Lauermann mot Österreichischer Rundfunk*).

6.2.4.2 Harmonisering

Direktivet er langt mer ambisiøst når det gjelder harmonisering av nasjonalt regelverk enn Europarådets konvensjon av 1981 og OECDs retningslinjer av 1980. Dette gjelder både fastsettelse av grunnprinsipper, begrepsapparat, tilsynsordninger og anvendelsesområdet for regulering. På visse punkter tillates likevel medlemsstater et «spillerom» ved implementering av direktivet. Bruk av relativt tvetydige formuleringer i flere av direktivets bestemmelser, samt lite rettspraksis fra EF-domstolen og andre toneangivende domstoler om hvorledes bestemmelsene skal tolkes, forsterker dette spillerommet. Harmoniseringsbestrebelsene i direktivet medfører dermed ingen fullstendig uniformering av nasjonale lover.

Direktivet er et såkalt minimumsdirektiv, dvs. det angir minstekrav som medlemsland må overholde. Medlemsland kan innføre en høyere grad av personopplysningsvern enn minstekravene, forutsatt at dette ikke strider mot direktivet som helhet (jf. spesielt bestemmelsen i artikkel 1(2) om fri flyt av personopplysninger innen EU/EØS).

6.2.4.3 Anvendelsesområdet

Anvendelsesområdet for direktivet omfatter både offentlig og privat sektor, men ikke virksomhet som faller utenfor fellesskapsrettens virkeområde (jf. artikkel 3(2)). Dette betyr at direktivet ikke omfatter virksomhet som er tilknyttet EUs andre og tredje «søyler» (jf. traktaten om europeisk union tittel V og VI), som behandling av personopplysninger «som gjelder offentlig sikkerhet, forsvar, statens sikkerhet (herunder statens økonomiske interesser når behandlingen er forbundet med spørsmål om statens sikkerhet) og statens virksomhet på det strafferettslige område» (jf. også fortalen nr. 13). Medlemsstater kan likevel velge å regulere slik virksomhet i samsvar med direktivets regler.

Behandling av personopplysninger som skjer «som ledd i rent personlige eller familiemessige aktiviteter» (jf. artikkel 3(2)) faller også utenfor direktivets anvendelsesområde. Det er videre tillatt å unnta behandling av personopplysninger fra mange av direktivets sentrale bestemmelser når dette er nødvendig for å sikre ytringsfrihet (jf. artikkel 9). Liknende unntak kan dessuten innføres når dette er nødvendig for å sikre bl.a. effektiv bekjempelse av kriminalitet, medlemsstatenes «vesentlige økonomiske eller finansielle interesser» eller «beskyttelsen av den registrertes interesser eller andres rettigheter» (jf. artikkel 13(1)).

6.2.4.4 Tilsynsordninger

Når det gjelder tilsynsordninger, krever direktivet at hvert medlemsland etablerer et eller flere uavhengige organer som skal føre tilsyn med implementeringen av nasjonalt regelverk på feltet (jf. artikkel 28(1)). Med visse unntak skal hvert medlemsland innføre en ordning med meldeplikt, som innebærer at behandlingsansvarlige må melde fra til vedkommende tilsynsorgan om behandling av personopplysninger forut for behandlingen (jf. artikkel 18 og 19). Det er tillatt med forhåndskontroll (også i form av konsesjonsplikt) av databehandling som «kan innebære særlige farer for de registrertes rettigheter og friheter» (jf. artikkel 20; jf. artikkel 28(3)). Forhåndskontroll skal imidlertid skje unntaksvis, ikke som hovedregel (jf. fortalen nr. 54).

Direktivet etablerer videre en arbeidsgruppe om personopplysningsvern (*Working Party on the Protection of Individuals with regard to the Processing of Personal Data*), som består av representanter fra nasjonale datatilsynsmyndigheter innenfor EU. Arbeidsgruppen er etablert i henhold til direktivets artikkel 29 og kalles derfor «artikkel 29 arbeidsgruppen». Arbeidsgruppens mandat er i hovedsak å gi Europa-kommisjonen råd om ulike problemstillinger angående personopplysningsvern, inklusiv nasjonal implementering av direktivet. Arbeidsgruppen har kun rådgivende myndighet, men er svært aktiv og har utstedt en lang rekke anbefalinger og veiledninger. Datatilsynsmyndighetene fra Norge og de andre EFTA-landene deltar i arbeidsgruppen som observatører uten stemmerett.

6.2.4.5 Grunnregler

Direktivet nedfeller en rekke grunnregler for behandling av personopplysninger som både viderefører og utvider prinsippene i Europarådets konvensjon fra 1981 og OECDs retningslinjer fra 1980. Dette gjelder spesielt regler om opplysningsplikt og innsynsrett (jf. artikkel 10-12). Direktivet etablerer i tillegg et par nye typer innsigelses-/reservasjonsrettigheter. For det første får enkeltpersoner rett til å motsette seg direkte markedsføring (jf. artikkel 14). For det andre får de en kvalifisert rett «til ikke å bli undergitt en beslutning som har rettsvirkning for vedkommende eller berører vedkommende i vesentlig grad, og som utelukkende er truffet på grunnlag av elektronisk behandling av opplysninger med sikte på å vurdere visse personlige forhold som arbeidsinnsats, kredittverdighet, pålitelighet, adferd osv.» (jf. artikkel 15(1)).

6.2.4.6 Overføring av personopplysninger til andre land

Mens overføring av opplysninger EU/EØS-medlemsland seg i mellom ikke kan begrenses av personvernhensyn (jf. artikkel 1(2)), er overføring av personopplysninger fra medlemsland til ikkemedlemsland (såkalte «tredjestater») underlagt forholdsvis strenge begrensninger. Overføring av personopplysninger til en tredjestat skal i utgangspunktet bare skje dersom staten «sørger for et tilstrekkelig vernenivå» (jf. artikkel 25(1)). Det finnes imidlertid en rekke unntak fra denne regelen, eksempelvis når den registrerte samtykker til overføringen eller overføringen er lovhjemlet eller nødvendig for inngåelse eller oppfyllelse av en kontrakt mellom den registrerte og den behandlingsansvarlige (artikkel 26(1)).

Europa-kommisjonen har kompetanse til å bestemme om en tredjestat tilbyr tilstrekkelig personopplysningsvern (jf. artikkel 25(6)), og kan i så fall overprøve medlemsstaters (og dermed nasjonale datatilsynsmyndigheters) egne vurderinger av tilstrekkelighet. Kommisjonen har så langt anerkjent kun et mindre antall land (deriblant Sveits, Argentina og Canada) som stater med et tilstrekkelig personopplysningsvern i henhold til artikkel 25. Systemet for tilstrekkelighetsvurderinger synes generelt å være nokså tregt og tungvint. Det er videre etablert flere ordninger som åpner for overføring av personopplysninger til visse organisasjoner i tredje stater (hittil hovedsakelig USA) som ellers ikke er ansett å tilby tilstrekkelig personopplysningsvern. Hovedeksempelet her er den såkalte «safe harbor» («trygg havn») ordningen, etablert i 2000, som innebærer at amerikanske selskaper vil kunne anses å tilby tilstrekkelig vern for personopplysninger som de mottar fra EU/EØS, ved at de frivillig implementerer et sett regler for behandling av opplysningene.

6.2.4.7 Rettspraksis

EF-domstolens praksis angående tolkning av direktivet er fremdeles sparsom, men har likevel fastslått flere grunnleggende trekk ved direktivet. De viktigste er at direktivet har en menneskerettslig (i tillegg til en markedsmessig) forankring og må derfor tolkes og anvendes i lys av EMDs praksis etter EMK (jf. særlig avgjørelse 2003-05-20 i sak C-465/00, *Rechnungshof mot Österreichischer Rundfunk m.fl.* og forente saker C-138/01 og C-139/01, *Neukomm og Lauermann mot Österreichischer Rundfunk*)).

Betydningen av EMK og EMDs praksis for anvendelse av direktivet er særlig sentral i avveininger mellom personvern og andre rettigheter der det må foretas proporsjonalitetsvurderinger. Dette gjelder ikke bare i forhold til direktiv 95/46 men også i forhold til andre EF-rettslige instrumenter vedrørende personopplysningsvern, så som direktiv 2002/58 om elektronisk kommunikasjon og personvern (jf. særlig avgjørelse 2008-1-29 i sak C-275/06 *Productores de Música (Promusicae) mot Telefónica de Espanã (Telefonica)*).

EF-domstolen har ellers elaborert enkelte aspekter ved direktivets anvendelse på publisering av personopplysninger på Internett (jf. avgjørelse 2003-11-6 i sak C-101/01, *Bodil Lindqvist*). Den har for det første fastslått at publisering av person-

opplysninger på en allmenntilgjengelig Internetthjemmeside faller innenfor direktivets anvendelsesområde; slik publisering kan ikke anses å være behandling av opplysninger «som ledd i rent personlige eller familiemessige aktiviteter» (jf. artikkel 3(2)). Domstolen har for det andre fastslått at slik publisering i seg selv utgjør nødvendigvis ikke en overføring av personopplysninger til tredjeland i henhold til artikkel 25.

6.2.5 Sektorvise direktiv

I tillegg til det generelle direktivet om personopplysningsvern har EU vedtatt to direktiv som omhandler personopplysningsvern i forhold til elektronisk kommunikasjon. Det ene er direktiv 2002/58/EF som gjelder elektronisk kommunikasjon generelt. Det inneholder regler om bl.a. sikring av data under kommunikasjon, lagring og viderebruk av trafikk- og debiteringsdata, utstedelse av spesifiserte regninger, fremvisning av anropende nummer hos oppringt sluttbruker, innholdet i abonnentfortegnelser, og forbud mot visse former for elektronisk søppelpost («spam»). Reglene er i hovedsak gjennomført i Norge ved loven om elektronisk kommunikasjon av 2003.

Det andre instrumentet er direktiv 2006/24/EF om lagring av trafikkdata generert i forbindelse med elektronisk kommunikasjon (*datalagringsdirektivet*). Det innebærer at EU-medlemsland må pålegge tilbydere av offentlige elektroniske kommunikasjonstjenester en plikt til å lagre trafikkdata i en periode på ikke mindre enn 6 måneder og ikke mer enn to år. Direktivets regler er ennå ikke implementert i Norge, og det er usikkert om direktivet er EØS-relevant. En nærmere redegjørelse for direktivet finnes i avsnitt 17.4.2. Personvernkommisjonens uttalelse om direktivet finnes som vedlegg 1.

Til slutt er det verdt å merke seg at EU arbeider med å få vedtatt harmoniserte regler om personopplysningsvern i politisektoren – en sektor under EUs tredje søyle. Dette arbeidet er ikke ferdig, og det pågår fremdeles debatt om reglenes innhold. Debatten dreier seg i hovedsak om hvorvidt Europarådets konvensjon om personopplysningsvern av 1981 eller direktiv 95/46/EF bør danne grunnlaget for slike regler.

6.2.6 Norges spillerom ved utforming av personvernregelverk

Selv om Norges frihet til å velge særnasjonale løsninger på feltet er redusert, har Norge fremdeles betydelig spillerom ved utforming av personvernregelverk og andre personvernfremmende tiltak. Dette gjelder i forhold til en rekke områder. Noen eksempler er:

- samtykkets innhold og rolle/status (for eksempel når skal innhenting av samtykke fra det registrerte være hovedvilkår for behandling av personopplysninger?);
- identifiseringsmekanismer (for eksempel når skal biometriske løsninger være tillatt?);
- integrering av personvernkrav i systemutvikling (for eksempel hvorvidt skal man kreve at nye informasjonssystemer tillater anonyme transaksjoner?)
- bruk og status av adferdskodekser (hvorvidt skal man oppfordre til utarbeidelse av disse? Hvilken rettslig status skal de få?).

Enkelte av disse spørsmålene er tatt opp i andre deler av rapporten.

Personvernkommisjonen ønsker ellers å understreke at alle dens forslag til personvernfremmende tiltak er forenlige med gjeldende folkerettslige krav på området.

Kapittel 7
Nasjonalt regelverk om personvern

I rapportens kapittel 4.1.5 har Personvernkommisjonen foretatt et skille mellom «personvern» og «personopplysningsvern». Personvern er knyttet til ivaretakelse av den personlige integritet, mens personopplysningsvernet gjelder bruk av opplysninger om enkeltpersoner. I norsk rett finnes det både bestemmelser som skal ivareta personvernet, slik som straffeloven § 390 og regler som har fokus på behandling av personopplysninger. Det er sistnevnte del av personvernretten som er underlagt den mest omfattende lovregulering, gjennom for eksempel personopplysningsloven, helseregisterloven og bestemmelser om taushetsplikt.

I dette kapittelet vil Personvernkommisjonen gi en oversikt over noen sentrale bestemmelser innenfor begge kategorier. I tillegg vil det ulovfestede personvernet berøres avslutningsvis. Det må presiseres at Personvernkommisjonen ikke har hatt anledning til å foreta en utfyllende beskrivelse av gjeldende rett. Fokuset er derfor rettet mot lovgivning som særlig har hatt relevans for kommisjonens arbeid. I tillegg til oversikten i dette kapittelet, vil personvernbestemmelser som har hatt særlig relevans innenfor de særskilte områdene kommisjonen har arbeidet med bli gjennomgått nedenfor, se del IV.

7.1 Personopplysningsloven

Personopplysningsloven er den generelle loven for behandling av personopplysninger i Norge. Loven trådte i kraft den 1. januar 2001 og erstattet personregisterloven fra 1978. Personregisterloven kom til anvendelse på opprettelsen av personregistre, det vil si registre eller fortegnelser der personopplysninger ble lagret systematisk. Den teknologiske utviklingen åpnet imidlertid for stadig nye muligheter til å behandle personopplysninger uten at det ble opprettet et register, og det var nødvendig med et nytt regelverk som var tilpasset dagens situasjon. Målet var å lage en teknologiuavhengig lov. Samtidig var Norge, gjennom EØS avtalen, forpliktet til å implementere EUs personverndirektiv (direktiv 95/46/EF), se kapittel 6.2.4.

Personregisterloven la opp til omfattende forhåndskontroll fra tilsynsmyndighetens side. Opprettelsen av personregistre som gjorde bruk av elektroniske hjelpemidler og andre registre med sensitive personopplysninger skulle ha konsesjon fra Datatilsynet, og nærmere regler for bruk av personopplysningene ble fastsatt gjennom vilkår i konsesjonen.

I personopplysningsloven er konsesjonsplikten begrenset til kun å gjelde for behandling av sensitive personopplysninger, også her med vidtgående unntak. I stedet bruker tilsynet mer av sine ressurser på etterkontroll, gjennom stedlige og brevlige tilsyn, og til råd og veiledningsvirksomhet. I tillegg inneholder personopplysningsloven flere materielle regler som styrer den konkrete behandlingen i stedet for at disse følger av konsesjon. Dette skaper bedre notoritet og forutsigbarhet for både den som bruker personopplysninger og den personopplysningene knytter seg til. Utover dette bygger imidlertid de to lovene på mange av de samme hensyn og personvernmessige prinsippene, slik at praksis etter personregisterloven vil stå sentralt også ved fortolkningen av personopplysningsloven.

7.1.1 Hovedtrekkene i personopplysningsloven

Personopplysningsloven gjelder behandling av personopplysninger med elektroniske hjelpemidler, samt opprettelse av manuelle personregistre. Spørsmålet om hva som skal anses som et «elektronisk hjelpemiddel» har vært drøftet av Personvernnemnda, se klagesak 2005/1. Nemnda fremhever at kravet om at det skal benyttes et elektronisk hjelpemiddel medfører at behandlingen må skje automatisk, uten intervensjon av mennesker.

Det finnes enkelte unntak fra lovens virkeområde. For kommisjonens arbeid er det særlig viktig å fremheve unntaket som regulerer forholdet til ytringsfriheten, se lovens § 7. Her er det be-

stemt at behandling av personopplysninger som skjer for kunstneriske, litterære eller journalistiske, herunder opinionsdannende formål, i hovedsak faller utenfor personopplysningslovens anvendelsesområde. I praksis medfører dette unntaket vanskelige avveininger mellom ytringsfrihet og personvern, noe kommisjonen vil beskrive nærmere i rapportens kapittel 13.

For all behandling av personopplysninger skal det utpekes en ansvarlig for behandlingen. I loven kalles dette den behandlingsansvarlige, og er definert som «*den som bestemmer formålet med behandling av personopplysninger og hvilke hjelpemidler som brukes*». Det er den behandlingsansvarlige som er pliktsubjekt etter loven og som er ansvarlig for at loven etterleves, herunder at den registrertes rettigheter ivaretas, se nedenfor. Ansvaret kan ligge hos både fysiske og juridiske personer.

Behandling av personopplysninger må oppfylle visse grunnkrav som følger av lovens § 11. Blant annet må det finnes et behandlingsgrunnlag, behandlingen må skje for et saklig begrunnet formål og opplysningene som brukes må være tilstrekkelige og relevante for å oppfylle dette formålet. I tillegg skal opplysningene være korrekte og oppdaterte og slettes når formålet er oppfylt.

Når det gjelder kravet om behandlingsgrunnlag, bety dette at ett av vilkårene i lovens § 8 må være oppfylt. Behandling av sensitive personopplysninger må i tillegg oppfylle ett av kravene i § 9. De alternative grunnlagene for behandling av personopplysninger er samtykke, lovhjemmel eller at behandlingen er nødvendig for å ivareta et av de nærmere definerte formål.

Alternativene i §§ 8 og 9 er etter ordlyden i utgangspunktet likestilte. Det følger imidlertid av forarbeidene at behandling av personopplysninger som ikke er hjemlet i lov, i størst mulig grad bør baseres på et samtykke fra den opplysningen knytter seg til (Ot. prp. nr. 92 (1998-99), side 108). Samtykke ivaretar vesentlige personverninteresser som selvbestemmelse og kontroll over egne opplysninger.

I Datatilsynets praksis har samtykket utviklet seg til å være den reelle hovedregel.[1] Dette har også blitt støttet av Personvernnemnda. I klagesak 2004/01 sier nemnda uttrykkelig at behandling av personopplysninger som hovedregel skal baseres på et samtykke.

For at et samtykke skal være gyldig, må det være frivillig, uttrykkelig og informert, se § 2, nr 8. Samtykkekravet reiser en rekke problemstillinger som Personvernkommisjonen vil berøre senere i rapporten. Blant annet gjelder dette samtykke fra barn og samtykke i arbeidslivet.

I tillegg til å dokumentere at det finnes et behandlingsgrunnlag og at øvrige grunnvilkår er oppfylt, har den behandlingsansvarlige en rekke andre plikter i personopplysningsloven. Det skal iverksettes nødvendige sikkerhetstiltak (§ 13) og utarbeides et system for internkontroll (§ 14) i tillegg til at melde- og konsesjonsplikten skal ivaretas (§§ 31 og 33). Som nevnt ovenfor er konsesjonsplikt i stor grad erstattet av meldeplikt, slik at det vil være opp til den behandlingsansvarlige selv å vurdere om lovens vilkår er oppfylt. Gjennom meldingen bekreftes at det er iverksatt tiltak som sikrer etterlevelse av loven, noe som eventuelt kontrolleres av Datatilsynet i ettertid. Med tanke på Datatilsynets begrensede ressurser, er det imidlertid få virksomheter som er gjenstand for kontroll årlig, sett i forhold til antall behandlinger som meldes inn. Som illustrasjon kan det nevnes at antall meldinger i 2007 var 2952, det ble gitt 237 konsesjoner og gjennomført 134 tilsyn.[2]

En ytterligere plikt for behandlingsansvarlige er å sørge for at den registrerte kan ivareta sine rettigheter. Disse er blant annet retten til informasjon (§ 19 flg.), innsyn (§ 18), retting og sletting (§§ 27 og 28). Informasjon og innsyn gir kontroll over hvilke personopplysninger som behandles til hvilke formål. Slik kunnskap er en nødvendig forutsetning for at den registrerte skal kunne påpeke feil eller mangler, kreve sletting og ellers kontrollere hvorvidt den behandlingsansvarlige etterlever sine plikter.

7.1.2 Datatilsynet og Personvernnemnda

Datatilsynet ble opprettet den 1. januar 1980 med hjemmel i den gamle personregisterloven. I dag finnes grunnlaget for Datatilsynets virksomhet i personopplysningsloven kapittel VIII. Datatilsynet er et uavhengig forvaltningsorgan. Det vil si at Kongen eller ansvarlig departement (Fornyings- og administrasjonsdepartementet) ikke kan instruere eller overprøve tilsynets beslutninger i enkeltsaker.

Datatilsynets oppgaver følger av personopplysningsloven § 42, 3. ledd, og knytter seg både til rene forvaltningsoppgaver, kontrollvirksomhet, råd- og veiledningsarbeid samt informasjonsvirksomhet. Datatilsynet fremhever ofte at deres ombudsfunksjon er vel så viktig som tilsynsfunksjo-

[1] Se blant annet sak med Datatilsynets referanse 2002/1683.

[2] Tallene er hentet fra Datatilsynets årsmelding for 2007

nen, og det å skape oppmerksomhet og interesse omkring personvernspørsmål står sentralt.

Det er Datatilsynet som fører tilsyn med mange av lovene som gir et personopplysningsvern i Norge. Deres kontrollvirksomhet omfatter både personopplysningsloven, helseregisterloven, helseforskningsloven og SIS-loven. I tillegg spiller Datatilsynet en sentral rolle ved tolkning av disse lovene gjennom sitt råd- og veiledningsarbeid. Av denne grunn er forvaltningspraksis, som rettskilde, av vesentlig betydning på personvernrettens område. Dette forsterkes ved at brudd på overnevnte lover i liten grad har vært gjenstand for domstolsbehandling, selv om flere av bestemmelsene er straffsanksjonert og brudd på disse kan utløse erstatningsansvar. Personvernkommisjonen vil berøre de mest sentrale rettsavgjørelsene og forvaltningspraksis der hvor dette er relevant, se særlig kapittel 13.2.3.

Klager over Datatilsynets avgjørelser behandles av Personvernenemnda, som har vært klageorgan for Datatilsynets vedtak siden den 1. januar 2001. Personvernnemnda er et uavhengig forvaltningsorgan som administrativt er underlagt Kongen og Fornyings- og administrasjonsdepartementet. Personvernnemnda har sju medlemmer som blir oppnevnt for fire år med adgang til oppnevning for ytterligere fire år.

Organiseringen av personvernmyndighetene vil bli nærmere drøftet i rapportens kapittel 18.

7.2 Personvernbestemmelser i særlovgivningen

7.2.1 Folkeregisterloven

Registrering av befolkningen er et gammelt fenomen, men systematisert, sentralisert og landsomfattende folkeregistrering ble først innført ved lov av 16. januar 1970 nr. 1. I dag registreres alle som er eller har vært bosatt i Norge, er født i Norge eller som har fått tildelt fødselsnummer (ev. D-nummer[3]) i Folkeregisteret. Ansvaret for registeret ligger hos Skattedirektoratet.

Folkeregisteret baserer sine opplysninger på lovpålagte meldinger fra borgerne og offentlige myndigheter, for eksempel i forbindelse med fødsel, bosetting, flytting og dødsfall. I forskrift om folkeregistrering er det listet opp hvilke opplysningstyper registeret inneholder.

Opplysninger i folkeregisteret om private forhold er underlagt taushetsplikt, jf. folkeregisterloven § 13. En rekke opplysninger som av mange anses for å være av privat karakter, anses ikke som «private forhold» i loven og kan utleveres både til private institusjoner og personer i tillegg til offentlige myndigheter, på visse vilkår. Dette gjelder for eksempel fødselsnummeret. Uten hinder av taushetsplikten kan det gis opplysninger til det offentlige, når dette er hjemlet i lov, til Statistisk sentralbyrå for utarbeidelse av statistikk og til forskning, jf. § 14.

De registrerte opplysningers kvalitet og ivaretakelse av konfidensialitet er to personverninteresser som står særlig sentralt når det gjelder folkeregisteret.

Opplysningene i folkeregisteret har stor betydning for offentlige myndigheter og danner grunnlaget for beslutninger om både tildeling av rettigheter og pålegging av plikter. Det er derfor viktig at registrerte opplysninger er korrekte og fullstendige. Med tanke på at opplysninger om hele landets befolkning er samlet i en sentral database, må konfidensialitet vektlegges. I denne sammenhengen er det nærliggende å vise til at ID-tyveri er en type kriminalitet som stadig øker i omfang, og at vår identitet i større grad har blitt en «råvare» for andre kriminelle aktiviteter. Dette er noe blant annet Datatilsynet har hatt særlig fokus på i de senere år (se Aanensen 2007).

7.2.2 Helseregisterloven

Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) trådte i kraft den 1.januar 2002. Også helseregisterloven bygger på prinsippene i EUs personverndirektiv (95/46/EF), men er en spesiallov for behandling av helseopplysninger i helseforvaltningen og helsetjenesten og for opprettelse av lokale, regionale og sentrale helseregistre. Behandling av helseopplysninger i medisinsk og helsefaglig forskning reguleres imidlertid av helseforskningsloven, se nedenfor. Personopplysningsloven supplerer helseregisterloven på viktige punkter, for eksempel når det gjelder kravene til informasjonssikkerhet.

Loven skal ivareta både personvernet, pasientinteresser og samfunnsinteresser. Som pasient i helsetjenesten er man nødt til å avgi en del helseopplysninger for å få adekvat helsehjelp. Samtidig må man ha tillit til at disse opplysningene oppbevares forsvarlig og at tilgangen er begrenset ut fra et tjenstlig behov. Samfunnets behov for tilgang til helsedata for å fremme folkehelseformål er ivare-

[3] Skattepliktige som ikke er bosatt i Norge får tildelt et D-nummer. Dette nummeret tildeles også andre ikke bosatte personer når norske myndigheter har behov for et entydig identifikasjonsbegrep.

tatt gjennom lovregulering av retten til å opprette helseregistre.

Helseregisterloven er bygd opp på samme måte som personopplysningsloven. Den databehandlingsansvarlige[4] har de samme pliktene som etter personopplysningsloven, herunder ansvar for at det finnes et behandlingsgrunnlag, etablering av internkontroll, informasjonssikkerhet og ivaretakelse av de registrertes rettigheter.

Helseregisterloven gir hjemmel for å opprette lokale, regionale og sentrale helseregistre. Behandling av direkte identifiserbare helseopplysninger i slike registre skal som hovedregel baseres på et samtykke fra den registrerte, med mindre opplysningene pseudonymiseres eller avidentifiseres. Helseregisterloven § 8 gir dessuten hjemmel for å lagre helseopplysninger i 9 sentrale helseregistre uten at det foreligger samtykke.

I mai 2008 ble loven tilføyd en viktig presisering hva gjelder tilgang til helseopplysninger. Det ble tatt inn et utrykkelig forbud mot å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helseopplysninger uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift. Se mer om dette i kapittel 16.4.3.3.

7.2.3 Helseforskningsloven

Lov om medisinsk og helsefaglig forskning (helseforskningsloven) ble vedtatt 20. juni 2008 og det er i skrivende stund ikke bestemt når loven skal tre i kraft. Loven gjelder for medisinsk og helsefaglig forskning på mennesker, humant biologisk materiale eller helseopplysninger. Formålet med loven er å fremme god og etisk forsvarlig forskning. Dette skal blant annet sikres gjennom krav til organisering, ansvar, åpenhet og innsyn, forhåndskontroll og tilsyn. I tillegg skal forsøkspersonens integritet og personvern ivaretas ved at det stilles krav om samtykke, informasjon og vurdering av hvilke fordeler og ulemper forskningen innebærer for samfunnet og enkeltindivider.

Loven flytter mye av ansvaret for forhåndskontroll med forskningsprosjekter fra Datatilsynet (behandling av helseopplysninger) og Sosial- og helsedirektoratet (dispensasjon fra taushetsplikt og tillatelse til opprettelse og bruk av forskningsbiobank) til de regionale komiteene for medisinsk og helsefaglig forskningsetikk. Dette medfører for eksempel at Datatilsynet ikke lenger skal gi konsesjon til forskning på helseopplysninger, da behandling av personopplysninger for slike formål nå har hjemmel i lov. De konkrete materielle reglene for denne behandlingen reguleres i hovedsak av helseforskningsloven.

De regionale etiske komiteene ble omgjort til forvaltningsorganer ved ikrafttredelsen av forskningsetikkloven, med Den nasjonale forskningsetiske komité for medisin og helsefag som klageinstans. Statens helsetilsyn og Datatilsynet er imidlertid gitt tilsynskompetanse innenfor sine respektive fagområder, jf. helseforskningsloven kapittel 9. Statens legemiddelverk godkjenner klinisk utprøving av legemidler i henhold til forskrift om klinisk utprøving av legemidler.

Helseforskningslovens virkeområde gjør den til en spesiallov for behandling av helseopplysninger i medisinsk og helsefaglig forskning i forhold til personopplysningsloven og helseregisterloven. Opprettelse av lokale, regionale og sentrale helseregistre reguleres fortsatt av helseregisterloven. Personopplysningsloven med forskrifter supplerer helseforskningsloven, blant annet når det gjelder krav til informasjonssikkerhet, jf. helseforskningsloven § 2, 3. ledd.

Ut fra personvernhensyn og i samsvar med generelle forskningsetiske prinsipper, stadfester loven at deltakelse i medisinsk og helsefaglig forskning skal baseres på et fritt, uttrykkelig og informert samtykke. I følge departementet var et klart lovkrav om samtykke nødvendig for å styrke forskningsdeltakernes rettsikkerhet (se Inst. O. nr. 55 (2007-2008), punkt 1.6.1). Det er imidlertid verdt å merke seg at det finnes en rekke unntak fra kravet om samtykke. Blant annet lempes det på kravet til informasjon gjennom bruk av såkalt brede samtykker (jf. § 14), og bruk av biologisk materiale som er innsamlet i en behandlingssituasjon skal kunne brukes til forskning uten samtykke, men med reservasjonsadgang (jf. § 28). Disse delene av lovforslaget har vært gjenstand for kritikk og diskusjon fra høringsinstanser og fagmiljøer.

7.2.4 Regelverk om politiets behandling av personopplysninger

Politiets behandling av personopplysninger er regulert i en rekke lover, forskrifter og instrukser. Generelt kan man si at også behandling av personopplysninger der politiet er ansvarlig, reguleres av personopplysningsloven. En viktig begrensning følger imidlertid av personopplysningsforskriftens § 1-3, som gir unntak fra personopplysningslo-

[4] Loven benytter et annet begrep enn behandlingsansvarlige for å skape et klarere skille mellom behandlingsansvarlig for opplysninger og det ansvaret helsepersonell har overfor pasienten i henhold til helselovgivningen.

vens virkeområde for saker som behandles eller avgjøres i medhold av rettspleielovene, herunder straffeprosessloven. Det er imidlertid ikke gitt at denne begrensningen gjelder behandling av opplysninger utenfor den konkrete straffesak, for eksempel nedtegnelse av opplysninger i sentrale og lokale registre som brukes i politiets saksbehandling. Dette vil bero på en konkret vurdering.

Personopplysningslovens anvendelsesområde vil også innskrenkes i den grad særlov regulerer behandlingsmåte, jf. personopplysningsloven § 5. Strafferegistreringsloven med forskrifter hjemler opprettelse av en rekke registre som brukes i politiets arbeid, blant annet: Det sentrale straffe- og politiopplysningsregisteret, BOT – det sentrale bøteregisteret og Krimsys. Straffeprosessloven gir hjemmel for opprettelse av registre med snevrere formål, som blant annet DNA-registeret og fingeravtrykkregisteret. Også her vil man måtte vurdere konkret om personopplysningsloven supplerer spesiallovene der disse ikke gir særskilte regler.

Sentral for politiets arbeid med kontroll ved landets yttergrenser er Lov om Schengen informasjonssystem (SIS-loven). Her hjemles behandling av personopplysninger i den norske delen av Schengen informasjonssystem (SIS) og utveksling av opplysninger mellom landene som deltar i Schengensamarbeidet, blant annet med det formål å forebygge og oppklare kriminelle handlinger. SIS-loven har bestemmelser som stiller krav til selve registreringen og ivaretakelse av den registrertes rettigheter.

I 2000 ble det nedsatt et utvalg som skulle utrede det rettslige grunnlaget for behandling av personopplysninger i politisektoren. Utvalget ga sin innstilling i NOU 2003:21. Behovet for ny lovgivning var blant annet begrunnet i at dagens regelverk var mangelfullt, og det ble stilt spørsmål ved om hjemmelsgrunnlaget for politiets registre tilfredsstiller kravene i EMK artikkel 8. Det pekes særlig på hensynet til tilgjengelighet og forutsigbarhet for de registrerte, sett i forhold til det inngrepet en registrering av opplysninger hos politi- og påtalemyndighet vil kunne medføre for borgerne. Utvalget viser også til at legalitetsprinsippet i norsk rett tilsier en klarere regulering av hvordan personopplysninger behandles i politisektoren, da den lovgivningen som hjemler dagens registre ikke inneholder klare bestemmelser om formål, lagringstid, ansvar, bruk etc. Etter det Personvernkommisjonen har fått opplyst, tar Justis- og politidepartementet sikte på å fremme et lovforslag våren 2009.

Behandling av personopplysninger hos politi- og påtalemyndighet, samt regulering av denne, innebærer en til tider vanskelig avveining mellom personvern og hensynet til kriminalitetsbekjempelse.

7.2.5 Arbeidsmiljølovens regler om kontrolltiltak på arbeidsplassen

Kontrolltiltak i arbeidslivet kan ha sitt grunnlag i teknologiske, økonomiske, sikkerhetsmessige, helsemessige og organisatoriske forhold. De favner om alt fra enkle tiltak for tidregistrering til inngripende tiltak som helseundersøkelser. Selv om behandling av personopplysninger i arbeidslivet reguleres av de generelle reglene i personopplysningsloven, har også arbeidsmiljøloven regler som setter vilkår for iverksettelse av selve tiltaket. Disse er gitt blant annet av hensyn til den enkelte arbeidstakers personlige integritet og er eksempler på personvernbestemmelser som favner videre enn det typiske «personopplysningsvernet».

Det rettslige utgangspunktet er at et kontrolltiltak som virker inngripende i forhold til arbeidstakers personlige sfære eller integritet ikke er rettsmessig med mindre det foreligger et rettslig grunnlag for tiltaket. Det skal foretas en avveining mellom begrunnelsen og behovet for kontrollen, kontrolltiltakets art og hvor inngripende det vil virke i forhold til den enkelte ansatte. Som et utgangspunkt kan man si at arbeidsgiver, i kraft av sin styringsrett, kan igangsette tiltak som er nødvendige for å lede, fordele og kontrollere arbeidet. Gjennom rettspraksis er det imidlertid utviklet generelle arbeidsrettslige regler og prinsipper som slår fast at kontrolltiltak skal ha saklig grunn og være forholdsmessige. Disse er nå nedfelt i arbeidsmiljøloven kapittel 9.

Arbeidsmiljøloven § 9-1 angir de generelle vilkår for arbeidsgivers kontrolladgang. Kontrolltiltaket må være saklig, både i forhold til virksomhetens art og overfor den som omfattes av tiltaket. Videre er det krav om at tiltaket ikke innebærer en uforholdsmessig belastning for arbeidstakeren. Arbeidsgiver plikter å drøfte behovet for, utformingen av og selve gjennomføringen av kontrolltiltaket med representanter for de ansatte, jf. § 9-2.

Arbeidsmiljøloven kapittel 9 har også enkelte særregler for noen spesielt inngripende, men samtidig praktiske tiltak, blant annet innhenting av helseopplysninger ved ansettelse og gjennomføring av medisinske undersøkelser av arbeidssøkere og arbeidstakere. Fra et personvernståsted er det verdt og merke seg at bestemmelsene gir en uttømmende oppregning av hvilke helseopp-

lysninger som kan innhentes og hvilke undersøkelser som kan iverksettes. Det kan således ikke innhentes samtykke til å gå utover de tilfeller som loven positivt hjemler.

Det rettslige utgangspunktet i arbeidslivet er utdypet i rapportens kapittel 15 under temaet «Personvern i arbeidslivet». Her har også Personvernkommisjonen gitt noen tilrådninger i forhold til to konkrete tiltak som særlig utfordrer arbeidstakeres personvern; arbeidsgivers innsyn i arbeidstakers e-post og elektroniske dokumenter samt varsling.

7.2.6 Vern mot offentlig meddelelse av personlige eller huslige forhold

Straffeloven § 390 verner privatlivets fred ved å gjøre det straffbart å gi offentlig meddelelse om personlige eller huslige forhold. Bestemmelsen kan sies å være en generell personvernbestemmelse som gjelder uavhengig av hvordan krenkelsen/meddelelsen skjer; både ytringer, skrift og bilder omfattes. I så måte favner bestemmelsen videre enn personopplysningslovens anvendelsesområde.

Krenkelse av privatlivets fred foreligger ved offentliggjøring (til allmennheten) av opplysninger som må sies å være av privat karakter. Kjerneområdet for bestemmelsen er vern mot formidling av sanne opplysninger om personlige forhold, men også usanne opplysninger omfattes. Usanne ytringer vil imidlertid også kunne rammes av straffelovens bestemmelser om ærekrenkelser, forutsatt at utsagnet er ærekrenkende, se nedenfor under kapittel 7.2.8. Omtalen trenger ikke være av negativ art, også positiv, men privat omtale omfattes.

Straffeloven § 390 medfører en begrensning i forhold til ytringsfriheten. Selv om den form for ytringer som § 390 omhandler i utgangspunktet er forbudt av hensyn til personvernet, må man ved tolkning av bestemmelsen ta i betrakning at også slike ytringer som hovedregel er vernet av grunnloven § 100 og EMK artikkel 10. Se mer om dette i kapittel 13.

7.2.7 Vern mot personfotografering og retten til eget bilde

Det finnes flere bestemmelser i lovverket som skal beskytte enkeltpersoner mot at det blir tatt bilde i gitte situasjoner og etterfølgende publisering/offentliggjøring av bildet.

Et bilde er en personopplysning i den grad en enkeltperson kan identifiseres (direkte eller indirekte). Publisering/offentliggjøring av bilder vil derfor kunne reguleres av personopplysningsloven i den grad dette skjer ved hjelp av elektroniske hjelpemidler og ellers omfattes av lovens virkeområde. Et eksempel her er publisering av bilder på hjemmesider. I praksis har det imidlertid vist seg at personopplysningsloven i flere tilfeller ikke kommer til anvendelse i saker som gjelder publisering av bilder, da man har ansett publiseringen for å ha et opinionsdannende formål. Se mer om grensen mellom ytringsfrihet og personvern i saker som gjelder publisering av bilder på Internett i rapportens kapittel 13.

Åndsverkloven § 45c er en personvernbestemmelse som forbyr gjengivelse eller offentliggjøring av bilder tatt av en person, med mindre det foreligger samtykke fra avbildede. I motsetning til personopplysningsloven, verner åndsverksloven også bilder av døde personer.

Det er en forutsetning at personen på bildet kan identifiseres, direkte eller indirekte, men ikke et krav om at allmennheten skal være i stand til å foreta en identifikasjon (Jongers 2006, s. 30ff).

Det er selve offentliggjøring av bildet som rammes av bestemmelsen. Krenkende eller plagsom adferd i forbindelse med at bildet blir tatt kan imidlertid være i strid med straffeloven § 390a.

Det er gjort viktige unntak fra retten til å bestemme over eget bilde i åndsverksloven § 45c, bokstav a-e, for eksempel av hensyn til ytringsfriheten, dersom bildet har aktuell og allmenn interesse. Allmennhetens informasjonsbehov må veies opp mot den avbildedes interesse i vern mot bruk av bilde i sammenhenger som er urimelig belastende. Se mer om denne avveiningen og redegjørelse for relevant rettspraksis i kapittel 13 om personvern og media.

En annen form for fotografering av enkeltpersoner er fjernsynsovervåkning, definert i personopplysningsloven som vedvarende eller regelmessig gjentatt personovervåkning ved hjelp av fjernbetjent eller automatisk virkende fjernsynskamera, fotografiapparat eller lignende apparat. Personopplysningsloven har regler både for adgangen til å fjernsynsovervåke og bruken av billedeopptak, se lovens kapittel VII.

Straffeprosessloven § 202a hjemler politiets adgang til å foreta skjult fjernsynsovervåkning på offentlig sted.

Domstolsloven § 131a forbyr fotografering, filmopptak og opptak for radio eller fjernsyn under forhandlingene i straffesaker og av siktede eller domfelte når vedkommende er på vei til eller fra rettsmøtet eller har opphold i den bygning hvor rettsmøtet holdes, med mindre det forelig-

ger samtykke. Retten kan gjøre unntak fra forbudet under hovedforhandling på visse vilkår.

I 1999 ble det vedtatt av denne bestemmelsen skulle erstattes av nye bestemmelser i domstolloven § 131 og straffeloven § 390c. Sistnevnte bestemmelse utvider fotograferings- og filmforbudet til også å gjelde mistenkte og vitner i bestemte situasjoner. Disse bestemmelsene har imidlertid ikke trådt i kraft, og Justisdepartementet har uttalt at utformingen av straffeloven § 390c vil bli gjenstand for ny vurdering (se St. melding nr 26 (2003-2004).

7.2.8 Vern av omdømme

Straffeloven §§ 246 og 247 verner om en persons æreføelse og omdømme, og representerer en avveining mellom ytringsfrihet og personvern. Bestemmelsen rammer rettsstridige ytringer, noe som innebærer at bestemmelsene må tolkes med de begrensninger som følger av blant annet EMK artikkel 10 og grunnloven § 100. Se mer om denne avveiningen og relevant praksis i kapittel 13.

Både ærekrenkelser i form av ord og handling omfattes og de kan være skriftlig eller muntlig fremført. I så måte gir bestemmelsene både et personopplysningsvern og et mer generelt vern av den personlige integritet. Det er en forutsetning at ytringen kan knyttes til en enkeltperson.

Ytringen er som hovedregel ikke straffbar dersom det føres bevis for at den er sann. Sanne ærekrenkelser vil imidlertid være rettstridige dersom de er fremsatt uten noen aktverdig grunn eller er utilbørlig på grunn av form, måten den er fremsatt på eller av andre grunner, jf. § 249, nr 2. Dersom utsagnet gjelder personlige eller huslige forhold, vil det også kunne rammes av straffeloven § 390, se ovenfor. Justisdepartementet arbeider med endringer av disse reglene, se omtale av dette nedenfor i kapittel 13.

Straffeloven § 135a gir vern mot diskriminerende eller rasistisk motiverte ytringer relatert til hudfarge eller nasjonal/etnisk opprinnelse, religion eller livssyn og homofil legning, leveform eller orientering.

7.2.9 Vern av konfidensialitet

Det finnes en rekke bestemmelser i lovverket som skal gi vern av konfidensialitet, det vil si motvirke at personopplysninger gjøres tilgjengelig for andre enn de som har lovlig tilgang.

Enkelte av bestemmelsene er knyttet til den situasjonen at man uberettiget skaffer seg tilgang til opplysninger, for eksempel bestemmelser om brevbrudd. I dag er denne bestemmelsen mest praktisk ved datainnbrudd. Andre bestemmelser gir forbud mot å videreformidle opplysninger man allerede har tilgang til, typisk regler om taushetsplikt.

I tillegg finnes det sikkerhetsmessige krav som har til formål å ivareta konfidensialitet, se særlig sikkerhetsbestemmelsene i personopplysningsforskriftens kapittel 2, § 2-11. Tilsvarende spesielle bestemmelser finnes innenfor spesifikke sektorer, for eksempel telesektoren. Ekomloven § 2-7 pålegger tilbydere av teletjenester å gjennomføre nødvendig sikkerhetstiltak for å verne om abonnentens kommunikasjon.

Privat kommunikasjon er blant annet beskyttet i straffeloven § 145 gjennom bestemmelsen om brevbrudd. Det er forbudt å skaffe seg uberettiget tilgang til innholdet av lukket skrift, som for eksempel brev, pakke etc. Det samme gjelder når opplysningene er lagret eller overføres ved elektroniske hjelpemidler.

Straffeloven § 145a forbyr avlytting eller opptak av telefonsamtaler eller samtaler man ikke selv deltar i. Dersom opptaket skjer ved hjelp av elektroniske hjelpemidler og enkeltpersoner lar seg identifisere, kan forholdet også rammes av personopplysningsloven.

Politiet har særskilte hjemler for kommunikasjonskontroll i straffeprosessloven kapittel 16a og 16b.

Ettersom kommunikasjon av personopplysninger er nødvendig for de fleste transaksjoner både i offentlig og privat sektor, er taushetsplikten et viktig ledd i den enkeltes kontroll med egne opplysninger. Taushetsplikt, enten den har sitt grunnlag i lov eller avtale, har som formål å sørge for at opplysningene ikke videreformidles til uvedkommende. Taushetsplikten kan være knyttet til at man besitter en bestemt stilling eller være av yrkesrelatert karakter.

Eksempelvis har alle som jobber i offentlig forvaltning taushetsplikt i henhold til forvaltningsloven § 13. Brudd på taushetsplikten er straffbart, jf. straffeloven § 121. Tilsvarende stillingsbestemt taushetsplikt gjelder som hovedregel for tilbydere av teletjenester i forhold til innholdet av elektronisk kommunikasjon, jf. ekomloven § 2-9.

Er man for eksempel helsepersonell av yrke, følger taushetsplikten av helsepersonelloven § 21. Her gjelder taushetsplikten for alle opplysninger man får i egenskap av å være helsepersonell, uavhengig av om man er i et tjenesteforhold. Konfidensialitetsvernet er ytterligere forsterket ved at det er

tatt inn et utrykkelig forbud mot å lese opplysninger man ikke har et tjenstlig behov for, jf. § 21a.

7.2.10 Sektorvise bestemmelser om anonymisering/sletting av personopplysninger

Generelt skal personopplysninger slettes når formålet med behandlingen (innsamlingen, lagring og bruk) er oppfylt, jf. personopplysningsloven § 28. Likestilt med sletting er anonymisering, det vil si at opplysningene ikke lenger kan knyttes til en enkeltperson. Slettekravet begrenser bruken av personopplysninger til det som er nødvendig og ivaretar således viktige personverninteresser som minimalitet og kontroll over egne personopplysninger.

I tillegg til det generelle slettekravet i personopplysningsloven, finnes en rekke konkrete slettekrav i særlovgivning. Et eksempel her er ekomloven § 2-7. Trafikkdata skal slettes eller anonymiseres når de ikke lenger er nødvendige for kommunikasjons- eller faktureringsformål. Her presiseres hvilke formål som styrer lagringstiden for opplysningene. I henhold til helsepersonelloven skal feilaktige eller misvisende og belastende opplysninger i journal som hovedregel slettes. I tillegg finnes det regler om oppbevaringstid og sletting i journalforskriften, jf. § 14. Mer konkrete slettfrister finnes i SIS-loven og SIS-forskriften. Opplysninger som er lagret i Schengen informasjonssystem skal slettes når formålet med registreringen er oppnådd. I forskriften er det imidlertid presisert at en absolutt slettefrist som hovedregel inntreffer etter tre år (§ 6-2), og for visse typer opplysninger allerede etter ett år (§ 6-3).

Det er verdt å merke seg at arkivloven vil sette vesentlige begrensninger for sletteplikten i offentlig sektor.

7.3 Ulovfestede regler

En beskyttelse av privatlivets fred og den personlige integritet, er også slått fast i et ulovfestet personvern. Disse domstolskapte prinsippene supplerer norsk lov, men kan også gi et selvstendig personvern og personopplysningsvern. Flere av de mest sentrale rettsavgjørelsene på personvernrettens område regulerer forhold som ikke tidligere var regulert i lov. Ikke sjelden har imidlertid slik praksis påvirket og blitt nedfelt i lovgivningen.

Allerede i 1896 ble retten til eksklusiv bruk av slektsnavn presisert av Høyesterett, se Rt 1896 s. 530 (*Aarsdommen*). Navn, som en personopplysning, ble således gitt et ulovfestet vern mot å bli tatt i bruk av andre enn en bestemt gruppe slektsmedlemmer, og en utenforstående mann ble fradømt retten til å bruke navnet Aars.

Et enda tydeligere eksempel på vern av privatlivet, finner vi Rt 1952 s. 1217 (*To mistenkelige personer*). Her var to personer brukt som modell for karakterene i en film. Disse var involvert i en mye omtalt kriminalsak, og den gjenlevende av forbryterne ønsket visning av filmen stanset. Han hadde sonet sin dom og etablert seg på nytt under et annet navn. Høyesterett ga mannen medhold under henvisning til det «alminnelige rettsvern for personligheten».

I forhold til en sentral personverninteresse, retten til innsyn, er Rt. 1977 s. 1035 (*Journaldommen*) illustrerende. En pasient krevde innsyn i sin pasientjournal. En slik rettighet var på det aktuelle tidspunktet ikke nedfelt i helselovgivningen slik det er i dag. Høyesterett ga mannen medhold under henvisning til «alminnelige rettsgrunnsetninger». Det er ikke presisert i dommen hvorvidt det er det ulovfestede personvern som legges til grunn for retten til innsyn, men en slik forståelse er innfortolket blant annet i juridisk teori, se for eksempel Schartum og Bygrave (2004, s. 253).

Lovligheten av fjernsynsovervåkning og bruk av billedopptak har også vært behandlet i en rekke rettsavgjørelser før man fikk utrykkelige regler om dette. Rt 1991 s. 616 (*Gatekjøkkenkjennelsen*) gjaldt spørsmålet om lovligheten av skjult fjernsynsovervåkning og bruk av opptak som bevis i straffesak. Eieren av et gatekjøkken mistenkte en av sine ansatte for å underslå penger fra kassa. For å sikre seg bevis for underslaget, koblet han en opptaker til et eksisterende videokamera som var satt opp i butikken for at de ansatte skulle kunne oppholde seg på spiserommet og samtidig se når det kom kunder inn i butikken. De ansatte ble ikke informert. I senere straffesak mot den ansatte ble billedopptaket nektet ført som bevis for underslaget. Høyesterett uttaler at måten beviset er fremskaffet på «*medfører et slikt inngrep i den personlige integritet at den ut fra alminnelige personvernhensyn i utgangspunktet bør anses uakseptabel.*» Videre uttaler Høyesterett at «*vesentlige personvernhensyn [taler for] at domstolene nekter bruk av bevis tilveiebrakt på denne måten. Ved en slik holdning vil domstolene motvirke denne form for krenkelser*».

I Rt 1990 s. 1080 (*Fotobokskjennelsen*) mente retten at et ulovfestet personvern *ikke* satte noen skranker for adgangen til å bruke et bilde tatt ved

automatisk trafikkontroll som bevis i en senere straffesak. Bildets opprinnelige formål var å dokumentere en fartsoverskridelse, men bildet avdekket også at mannen hadde tyvegods på lasteplanet. Som forsvar for mannen ble det anført at bildet ikke skulle brukes til andre formål en trafikkovervåkning, senere formulert som det såkalte formålsbestemthetsprinsippet. Høyesterett la imidlertid større vekt på at bildet var fremskaffet på lovlig måte og at mannen var informert om fotograferingen via skilting.

På arbeidsrettens område har ulovfestet personvern blitt anført en rekke ganger som skranke for arbeidsgivers iverksettelse av kontroll- og overvåkningstiltak.

I RG 1993 s. 77 (*E-postdommen*) henviste retten til det ulovfestede personvern når de vurderte om arbeidsgiver hadde adgang til å overvåke/gjøre innsyn i en ansatts private område på virksomhetens datasystem i forbindelse med en oppsigelse. Det henvises til at innsyn innebar en krenkelse av de krav en arbeidstaker har på beskyttelse av privat informasjon.

Tilsvarende problemstilling var oppe Rt 2001 s. 1589 (*Raufossaken*). Her kontrollerte arbeidsgiver en ansatts internettbruk via loggfilen, da vedkommende var mistenkt for å ha lastet ned et betydelig antall musikkfiler. Arbeidsgiver skaffet seg også adgang til den ansattes PC og tok utskrift av harddisken. I dommen ble det vurdert hvorvidt bedriften har overtrådt det lovfestede og ulovfestede personvernet gjennom disse kontrolltiltakene, men man kom til at innsyn var rettmessig i det konkrete tilfellet.

7.4 Revisjon og etterkontroll av regelverket

I Ot.prp nr. 92 (1998-99) ble det forutsatt at personopplysningsloven skulle revideres etter ca. fem år. En totalrevisjon av lovverket er ikke gjennomført fra Justisdepartementets side, men det er igangsatt diverse forarbeid som ledd i en slik etterkontroll. Blant annet ble professor dr. juris Dag Wiese Schartum og førsteamanuensis dr. juris Lee A. Bygrave ved Det juridiske fakultet, Universitet i Oslo, gitt i oppdrag å utrede behovet for endringer i loven i forhold til sentrale temaer, se Schartum og Bygrave (2006). Hovedkonklusjonen i rapporten er at det er behov for omfattende endringer i dagens lov.

Norsk Regnesentral har gjort en utredning i forhold til elektroniske spor (Danielsson et al. 2005).

Høsten 2008 fremmet Justisdepartementet forslag om enkelte endringer i personopplysningsloven i Ot.prp. nr. 71 (2007-2008). Departementet forslår å gi hjemmel for forskrifter om særskilte former for behandling av personopplysninger, hjemmel for at Datatilsynet kan ilegge overtredelsesgebyr samt hjemmel for innkreving av tvangsmulkt, overtredelsesgebyr og refusjonskrav ved Statens innkrevingssentral. Forskriftshjemmelen er i første rekke ment å skulle brukes til å gi forskrifter om arbeidsgivers innsyn i ansattes e-post. Se mer om dette i kapittel 15.4.2.

Fornyings- og administrasjonsdepartementet, som er ansvarlig departement for personopplysningsforskriften, har vedtatt mindre endringer i denne. Blant annet i forhold til overføring av personopplysninger til utlandet og unntak fra melde- og konsesjonsplikten.

Når det gjelder andre lovarbeider som er relevante på personvernrettens område, kan det nevnes at Justisdepartementet arbeider med å revidere straffelovens regler om ærekrenkelser og vern av privatlivets fred. I høringsbrevet foreslås det å innta et krav om at ærekrenkelsen må være grov, både når det gjelder krenkelse av æreføelsen og krenkelse av omdømmet. En slik begrensning finnes ikke i gjeldende rett. I høringsbrevet (Borvik 2008b) fremheves det at nasjonal lovgivning som skal gi vern mot ærekrenkelser og krenkelser av privatlivet må utformes på en måte som ivaretar både hensynet til EMK artikkel 10 og EMK artikkel 8. I forhold til bestemmelser om krenkelse av privatlivets fred, ønsker departementet å slå sammen straffeloven § 249 nr 2 og straffeloven § 390, slik at det straffbare knytter seg til det å krenke privatlivets fred ved å gjøre private forhold *offentlige.* Se mer om dette i kapittel 13.

Av mandatet følger det at Personvernkommisjonens skal gi en helhetlig status over utfordringene for personvernet, herunder om dagens regelverk og andre virkemidler er egnet til å ivareta personvernet i dagens samfunn. Kommisjonen skal likevel ikke fremme konkrete lovforslag eller ta stilling til konkrete spørsmål om lovgiving som faller inn under det pågående arbeidet med etterkontroll av personopplysningsloven som skjer i regi av Justisdepartementet.

I sitt arbeid har Personvernkommisjonen avdekket flere svakheter ved det regelverket som er fastsatt for å gi et personopplysningsvern og personvern i Norge. Disse er påpekt og drøftet under de særskilte områdene kommisjonen har arbeidet med, se rapportens del IV. Her vil vi fremheve noen av de mest sentrale utfordringene.

Under temaet personvern og media påpeker kommisjonen svakheter i forhold ansvarsforholdene ved bruk av nye medietyper og medieroller. Slike uklarheter kan være til skade for personvernet da det skaper usikkerhet i forhold til hvem som kan gjøres ansvarlig i forhold til ulovlige ytringer. Konkret anbefaler Personvernkommisjonen at det utarbeides en medieansvarslov som omfatter alle media, og som klargjør hvem som er ansvarssubjekt i media som i sin art er uten en typisk redaktør.

Videre har Personvernkommisjonen pekt på at tolkningen av åndsverksloven § 45 c synes å skape usikkerhet i praksis, og at bestemmelsen bør revideres med henblikk på hvordan retten til eget bilde skal forstås i lys av nasjonal og internasjonal rett.

Når det gjelder offentliggjøring av skattelistene, mener et flertall i Personvernkommisjonen at personvernhensyn tilsier en innsnevring av dagens praksis. Flertallet mener at det er viktig av hensyn til samfunnsdebatten at skattelistene er tilgjengelige både for publikum og mediene. For å hindre misbruk, bør slik tilgang imidlertid kun skje på Skatteetatens nettsider, og mulighetene til søk og sammenstilling bør være begrenset.

Kommisjonen har også pekt på at det er behov for revisjon av dagens regler om pliktavlevering av elektronisk materiale til Nasjonalbiblioteket, da personvernhensyn ikke synes godt nok ivaretatt ved dagens ordning.

Under temaet personvern for barn og unge har Personvernkommisjonen identifisert klare svakheter ved dagens rettslige regulering når det gjelder ivaretakelse av barns personvern. Dette gjelder for eksempel i forhold til hvem som skal utøve rettighetene; foreldrene, barnet, barnet og foreldrene i felleskap, noe som viser seg særlig i forhold til spørsmål om samtykke til publisering av bilder på Internett. Personvernkommisjonen forslår en presisering av regelverket som gjelder publisering av barns personopplysninger.

Videre etterlyser kommisjonen konkrete regler om innhenting og bruk barns personopplysninger til bruk for markedsføringsformål.

Under temaet personvern i arbeidslivet har Personvernkommisjonen avdekket svakheter når det gjelder plassering av reglene som skal ivareta arbeidstakeres personvern. Disse er spredt både over flere lover og ulike rettsområder. Personvernkommisjonen etterlyser et helhetlig regelverk som tydelige angir grensene for arbeidssøkeres og arbeidstakeres integritetsvern, personvern og personopplysningsvern. Kommisjonen mener det bør vurderes å utarbeide en egen lov om personvern i arbeidslivet.

Under temaet personvern i helsesektoren, har Personvernkommisjonen påpekt at det må iverksettes tiltak som sikrer at regelverkets bestemmelser om taushetsplikt ivaretas i praksis. Dette gjelder både i forhold til kommunikasjon med pasienten, internt i virksomheten og mellom virksomheter. Det må stilles konkrete krav til systemer som håndterer pasientinformasjon, og bestemmelsene om taushetsplikt må gjennomgås med tanke på å evaluere hvorvidt dagens regelverk samlet sett innebærer en tilstrekkelig ivaretakelse av sentrale personvernhensyn.

Når det gjelder den rettslige reguleringen av sentrale helseregistre, mener Personvernkommisjonen at det er behov for en gjennomgang av eksisterende hjemler. Det bør vurderes om registrene fungerer hensiktsmessig etter sitt formål, om det var nødvendig å opprette registeret i forhold til det anførte formålet og om personvernhensyn blir tilfredsstillende ivaretatt ved den etablerte registerformen.

Under temaet personvern i transport- og kommunikasjonssektoren, har Personvernkommisjonen påpekt at man må legge større vekt på personvernrettens krav til proporsjonalitet ved innføring av personverninngipende tiltak innen kommunikasjon og transport.

Når det gjelder datalagringsdirektivet, mener kommisjonen at både politiets og andre nasjonale myndigheters behov for utvidet lagring og tilgang til trafikkdata i det omfang som er foreslått, må begrunnes bedre. Personvernkommisjonen finner ikke å kunne støtte innføring av direktivet uten at behovet for utvidet lagring er bedre dokumentert.

Videre påpeker Personvernkommisjonen at det hefter usikkerhet i forhold til hvordan dagens regelverk regulerer bruken av automatiserte registreringsenheter som er innebygd i ulike produkter. Kommisjonen mener det må utredes hvordan nåværende regelverk (inklusiv personopplysningsloven) løser slike spørsmål og hvorvidt regelverket bør endres for bedre å fremme personvernhensyn ved produksjon og bruk av data i slike tilfeller.

7.5 Grunnlovsfesting av personvernet

Selv om personopplysningsvernet og det mer generelle personvernet er godt forankret i norsk lov-

givning og anerkjent på ulovfestet grunnlag, har Personvernkommisjonen vurdert om det foreligger behov for en grunnlovfesting av personvernet i Norge. Per i dag er det få bestemmelser i Grunnloven som gir noen direkte beskyttelse av personverninteresser. Et eksempel er Grunnloven § 102 som forbyr husinkvisisjoner bortsett fra i «kriminelle tilfeller». Indirekte kan man også si at personvernet, som menneskerettighet, har et visst grunnlovsvern ved at staten er forpliktet til å respektere og sikre menneskerettighetene gjennom Grunnloven § 110c.

Spørsmålet om grunnlovsfesting blir stadig aktualisert ved den formelle anerkjennelsen og utbyggingen av personvernrettigheter som skjer internasjonalt gjennom folkeretten. Styrking av ytringsfriheten gjennom endringen av Grunnloven § 100 i 2004, har også aktualisert behovet for en grunnlovsbestemmelse som presiserer betydningen av personvernet i norsk rett. Grunnloven har stor rettslig og politisk betydning, i tillegg til at den har en vesentlig symboleffekt både for borgerne og staten. Grunnlovsfesting av personvernet vil medføre at personvernet får en sentral rolle i konkrete saksforhold, samtidig som man presiserer at også individuelle rettigheter er en viktig del av vår rettstat.

Personvernkommisjonen drøfter temaet Grunnlovsfesting av personvernet i kapittel 19 og anbefaler at personvernet, herunder retten til privatliv og personopplysningsvernet grunnlovsfestes i Norge.

7.6 Er regelverket om personvern vanskelig tilgjengelig?

Ved innføringen av personopplysningsloven fikk man som nevnt flere materielle regler i selve lovteksten. Dette skulle skape tilgjengelighet og forutsigbarhet for både den registrerte og den som registrerer, men forutsetter også at partene har en aktiv tilnærming til lovverket og de rettigheter og plikter som kan uledes av dette.

I praksis har det vist seg at personopplysningsloven er vanskelig tilgjengelig for begge parter, særlig fordi flere av bestemmelsene er svært skjønnsmessig utformet og legger opp til vanskelige interesseavveininger. To undersøkelser som ble gjennomført av Transportøkonomisk institutt på oppdrag fra daværende Moderniseringsdepartementet (nå Fornyings- og administrasjonsdepartementet) og Datatilsynet, kan sies å underbygge denne påstanden.

Den ene undersøkelsen rettet seg mot behandlingsansvarlige, og hadde blant annet til formål å undersøke hvorvidt virksomheter hadde kunnskap om og etterlevde kravene i personopplysningsloven. Konklusjonen var at behandlingsansvarliges kunnskap om loven og de pliktene som følger av den, er lav, og bare et mindretall oppfyller lovens krav (Ravlum 2005a).

Den andre undersøkelsen rettet seg mot enkeltpersoner – de registrerte, og hadde befolkningens holdning til og kunnskap om personvern i fokus (Ravlum 2005b). Konklusjonen var at de fleste har stor tillit til at personvernet blir ivaretatt på en god måte. De er ikke er særlig bekymret for at personopplysninger kan bli misbrukt. En stor andel reflekterer ikke over at det blir samlet inn opplysninger om dem, eller de bryr seg ikke om det. Mange av oss gir fra oss opplysninger vi egentlig ikke ønsker å gi. Som det fremheves av forfatterne gir dette grunn til «*å sette spørsmålstegn ved forutsetingen om at folk i stor grad skal ivareta sitt eget personvern*».

En annen faktor som har betydning for graden av tilgjengelighet er regulering av sentrale personvernbestemmelser i forskrift. Særlig personopplysningsforskriften har flere viktige materielle regler som regulerer den behandlingsansvarliges plikter og den registrertes rettigheter. Som eksempel kan nevnes detaljerte bestemmelser knyttet til informasjonssikkerhet, unntak fra melde- og konsesjonsplikt samt fjernsynsovervåkning. Generelt er det grunn til å tro at bestemmelser i forskrift er mindre tilgjengelige enn regler nedfelt i selve loven. Forskrift kan imidlertid være velegnet for detaljregulering innenfor spesifikke bransjer/sektorer, da man kan forvente at personvernbestemmelser som har betydning innenfor et særskilt livsområde er bedre kjent for den gruppen de gjelder.

Det må i denne forbindelse bemerkes at personopplysningslovens og forskriftens skjønnsmessige utforming har sammenheng med at de i prinsippet gjelder innenfor alle sektorer og bransjer hvor personopplysninger behandles. Et altfor konkret lovverk kan føre til at loven får et for snevert anvendelsesområde i praksis og ikke er egnet til å løse konkrete problemstillinger.

Utfordringer knyttet til et spredt og fragmentarisk lovverk mener Personvernkommisjonen vil kunne avhjelpes ved at man utarbeider særskilte regelverk om personvern innenfor konkrete bransjer og sektorer. Arbeidslivet er et godt eksempel her, se mer om dette i kapittel 15.

7.7 Ivaretakelse av personvernhensyn ved implementeringen av nye lover

Høsten 2008 publiserte Fornyings- og administrasjonsdepartementet en veileder i vurdering av personvernkonsekvenser som er ment å være et vedlegg til Utredningsinstruksen (FAD 2007). Formålet med veilederen er å bidra til at statlige etater på en god måte kan utrede de personvernmessige konsekvensene av sine forslag. Personvernkommisjonen mener at veilederen er et viktig bidrag for ivaretakelse av personvernet.

Personvernkommisjonen mener videre at en Grunnlovsfesting av personvernet vil kunne styrke vektleggingen av personverninteresser når man vedtar nye lover og i lovgivningsprosessen, se kapittel 19.

Del III
Det teknologiske landskapet

Kapittel 8
Innledning

I en dissens til dommen *Olmstead mot USA* (277 U.S. s. 438, 1928), setter dommer Louis Brandeis (1856-1941) søkelyset på den rollen som teknologi og vitenskapelige fremskritt spiller i forhold til å få tilgang til informasjon som den enkelte ønsker å holde skjult:

> «Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack to obtain disclosure in court of what is whispered in the closet. The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.»

I *Eit informasjonssamfunn for alle* (St.meld. nr. 17, 2006-2007, s. 137) peker FAD på at tilgang til slik teknologi ikke lenger er forbeholdt staten og mektige organisasjoner, men i dag også er tilgjengelig for privatpersoner:

> «Samtidig som det skjer ein auka bruk av personopplysningar innan politi- og påtalemakt, offentleg forvaltning og tenesteyting, kommersiell verksemd mv., er ein del nye teknologiar òg tilgjengelege for privatpersonar som kan bruke desse til å overvake eller spore andres daglegliv. Allmenta sin tilgang til Internett, mobiltelefoni med kamera mv. gjer at personvernet ikkje berre er truga av mektige organisasjonar, men også av «naboen».»

Ny teknologi for å samle inn og analysere personlige opplysninger dukker stadig opp. Mange av disse nye teknologiene for overvåkning, sporing og analyse favner videre, og pløyer dypere, enn tidligere, og overskrider de naturlige barrierene (f.eks. vegger, hud, mørke, tid og rom), som tidligere utgjorde hindre mot overvåkning og sporing. Disse teknologiene forbedres og raffineres dessuten hele tiden, både kvantitativt og kvalitativt. Kvantitative fremskritt muliggjør *mer* overvåkning av *flere* individer. Kvalitative fremskritt muliggjør en overvåkning som både er *mer usynlig* og *mer effektiv* enn tidligere.

Samtidig arbeides det med å utvikle teknologi som fremmer personvernet. Dette kan for eksempel være teknologi som forsøker å verne informasjon mot uønsket innsyn, eller teknologi som ved å skape «avstand» mellom en person og opplysninger om personen, gjør personopplysningene mindre identifiserbare.

En viktig drivkraft bak denne utviklingen, som nå har pågått i mer enn førti år, er en stadig mer omfattende *digitalisering* av informasjon, sammen med økende og stadig billigere beregningskapasitet.

Digitaliseringen omfatter alle mulig slags generelle personopplysninger (f.eks. hvem vi er, hva vi gjør, hvor vi befinner oss), og mer spesifikke personopplysninger om vår genetiske sammensetning, hentet fra molekylærbiologien. Personvernet utfordres når slike digitale data samles inn og gjøres tilgjengelig i databaser for gjenfinning, søking, sekvensering og strategisk informasjonsanalyse.

Tidligere ble vårt privatliv i en viss grad beskyttet av teknologiske begrensninger. Det var rett og slett ikke praktisk og økonomisk mulig å lage genetiske profiler over store deler av befolkningen, eller å samle inn enorme mengde personopplysninger om hver enkelt av oss og strukturere disse opplysningene på en meningsfylt måte.

Disse begrensningene er i ferd med å forsvinne. Det er særlig teknologiske fremskritt på områdene IKT og bioinformatikk som gjør det teknisk og økonomisk mulig for staten, bedrifter, og endog for privatpersoner å overvåke, spore, lagre og analysere stadig mer elektronisk kommunikasjon og stadig flere elektroniske spor og biologiske spor.

Forbedringene innenfor molekylærbiologi har blant annet gjort oss langt mer sporbare i den fysiske verden, fordi det er nesten umulig å opphold e seg et sted uten å legge igjen DNA.

Når det gjelder vår adferd og våre bevegelser i kyberrommet, innebærer vår utstrakte og entusiastiske bruk av digitale tjenester at vi også der er sporbare.

Til sammen innebærer altså det kjølvannet av biologiske og elektroniske spor som vi etterlater oss, sammen med tilgangen på billig beregningskraft, at det er mulig for de som måtte ha interesse av dette å få tilgang på langt mer data om hver enkelt av oss og våre bevegelser, enn noen gang tidligere. Og fordi et av teknologiutviklingens bidrag hele tiden er å øke kapasiteten og redusere kostnadene, er presset fra den teknologiske utviklingen på personvernet i dag større enn noen sinne.

Eksempler på denne typen press ser vi blant annet i form av statlige tiltak som EUs datalagringsdirektiv, det britisk-amerikanske ECHELON-systemet (Bye og Sjue 2008, ss. 234-242) og den svenske FRA-loven (Hannemyr 2008a), samt gjennom presset på å få opprettet stadig flere omfattende registersystemer (nasjonalt DNA-register, pasientregister, elevregister) med innsamling og langtidslagring av stadig flere personopplysninger og biologiske opplysninger.

Vi ser det også i privat sektor, blant annet i form av teknologier som for eksempel lojalitetskort (bonuskort), informasjonskapsler («cookies») og RFID-brikker. En tydelig trend de siste årene er «gratis» tjenester der forretningsmodellen i realiteten er at personopplysninger anvendes som bytte- og betalingsmiddel (eksempel: Google, Facebook).

Til sist ser vi det helt nede på det personlige plan. Internettsøk («googling»), der man kan taste inn navnet på en slektning, kollega, arbeidssøker eller nabo og øyeblikkelig få tilgang til alle de nettsider der vedkommende er omtalt eller selv har ytret seg, er bare ett av de moderne fenomenene som har økt eksponeringen til de fleste av oss dramatisk. I tillegg selges det nå avansert teknologi som gjør det mulig for blant annet sjalu ektefeller og bekymrede foreldre å overvåke makers og barns PC-er og mobiltelefoner, og å overvåke bevegelsene til de som bærer slikt utstyr med seg.

Digitaliseringen og rikelig tilgang på rimelig beregningskapasitet er imidlertid en nødvendig forutsetning for å kunne ta i bruk systemer for identitetsforvalting. Det samme gjelder for muligheten til å ta i bruk sterk kryptografi, som et mottrekk mot signalovervåkning.

Teknologiens inngrep i forhold som angår personvernet er svært omfattende. En uttømmende fremstilling av dette har det ikke vært realistisk å få til innenfor de rammene kommisjonen har hatt for sitt arbeide – kanskje ikke engang realistisk uansett rammer, fordi man på dette området skyter på et bevegelig mål.

Det man finner i denne delen av rapporten, er noen eksempler på hvordan personvernet utfordres, påvirkes, og eventuelt fremmes av den teknologiske utviklingen og av vitenskapelige fremskritt.

De teknologiske feltene som primært kommer til å gjøre inngrep i personvernet er molekylærbiologi og IKT (informasjons- og kommunikasjonsteknologi). Samtidig kommer fremskritt på disse fagfeltene til å resultere i forhold som har en rekke positive ringvirkninger, inklusive:

- økt effektivitet og lavere kostnader i produkter og tjenester, særlig når det gjelder transport og lagring av data,
- bedre sikkerhet i forretningsliv og offentlig virksomhet,
- bedre forbygging og etterforskning av kriminalitet og terror,
- genterapi, bedre helsetjenester,
- mange andre nye produkter og tjenester.

Personvernhensynet blir altså i økende grad gjenstand for en avveining der ulike hensyn settes opp mot hverandre. Man kan frykte at hensynet til personvernet blir vanskelig å ivareta fordi de samfunnsmessige positive effektene av å bruke ny teknologi, blir vektlagt som et tungt hensyn.

Personvernkommisjonen mener derfor at det er viktig å slå fast at personvernet er en menneskerettighet som ikke kan relativiseres.

For å sikre personverninteressene mener Personvernkommisjonen at når ny teknologi introduseres i samfunnet, bør som hovedregel teknologiens innvirkning på personvernet utredes på lik linje med teknologiens innvirkning på miljø og økonomi. For teknologier som forholder seg til biologiske og elektroniske spor, er det særlig grunn til varsomhet, og det må legges klare føringer for hvordan og i hvilken utstrekning slike spor kan lagres, behandles og slettes.

Tidligere har det ofte vært kostnadsmessige skranker for hvor mye data som kan samles inn, behandles, transporteres og lagres. Disse økonomiske begrensningene er nå i ferd med å forsvinne. I mange tilfeller er det rimeligere for en virksomhet å lagre alt den samler inn av data permanent, fremfor å bruke ressurser på å sortere ut det som bør slettes. Vi er på vei inn i en verden der ingen informasjon forsvinner «av seg selv». Dette er i seg selv et problem, og i tillegg fører det

til dårligere datakvalitet ved at utdatert informasjon og feilinformasjon overlever i ymse registre. Derfor må samfunnet legge føringer for hva som skal lagres og hva som skal slettes.

Vi vil være vitne til en økning i utveksling av elektronisk informasjon mellom organisasjoner og mellom enkeltpersoner i de kommende årene. Utviklingen innen massemedia, e-handel og e-forvaltning vil være de viktigste årsakene til dette. Dette vil virke effektiviserende på en rekke områder, samtidig som det representerer nye muligheter og nye arenaer for misbruk. Behovet for å beskytte dataene som strømmer i nettverkene vil øke tilsvarende. Dette vil avstedkomme videre utvikling av teknologier for kryptering, utarbeidelse av spesielle sikkerhetssertifikater og innføring av elektroniske signaturer.

Utnyttelse av IKT betyr en effektiviseringsmulighet i samfunnet. Teknologien er imidlertid ikke så robust at den ikke kan settes ut av spill. Kommunikasjonsenheter kan forstyrres. Databaser kan stjeles eller ødelegges. Personopplysninger kan komme på avveie.

Den allmenne bruken av IKT som er vanlig i vårt samfunn, skaper en rekke utfordringer i forhold til personvernet som knytter seg til bruken av personlige datamaskiner og tilhørende programvare. Dette omfatter blant annet:

- Skadelig programvare (*malware*) på den enkeltes personlige datamaskin som avlytter maskinen (*spyware*), eller som utfører kompromitterende handlinger (for eksempel planter falske bevis), eller som på andre måter krenker personvernet. Slik skadelig programvare kan bli plassert på datamaskinen via sikkerhetshull i operativsystemet eller nettverksforbindelsen, via e-post-vedlegg, eller automatisk via et nettsted brukeren besøker.
- Datainnbrudd og datasnoking (*hacking*). Dette omfatter både bruk av teknologi og bruk av sosial manipulering (dvs. bruk av sosiale metoder for urettmessig å få tilgang til blant annet adgangskoder til datamaskiner og datasystemer).
- Identitetstyveri (ofte formålet med *malware* og *hacking*).
- Cookies (har også legitime formål, men kan også utnyttes til sporing og ulovlig informasjonsinnsamling, m.m.) og webbugs (har ingen legitime formål).
- Facebook/Google og andre vanlig brukte brukerprogrammer som «bytter» personopplysninger mot tjenester.
- Systematisk og ulovlig innsamling av navn og e-postadresser for markedsføringsformål (dvs. for utsendelse av såkalt «spam»).
- Software og utstyr for å samle inn informasjon og trekke ut etterspurte data (sjekke ansatte, bedrifter eller privatpersoner).
- Distribusjon av krenkende informasjon og bilder på Internett av tredjepart.

Kapittel 9
Teknologiske trender som utfordrer personvernet

Molekylærbiologi og informasjons- og kommunikasjonsteknologi kommer sannsynligvis til å spille en viktig rolle som *drivkraft* i utviklingen av samfunnet. Innenfor disse områdene vil vi i årene som kommer oppleve at en rekke nye tjenester og produkter utvikles og anvendes på ulike områder i samfunnet.

Det er imidlertid viktig å være klar over at verken retningen eller hastigheten på denne drivkraften alene bestemmes av vår evne til nyskapning. Det er ikke slik at teknologien vil bli benyttet til alt det er mulig å bruke teknologien til. Som handlende og politiske mennesker har vi mulighet til å påvirke hvordan teknologien blir brukt. Det er ikke alltid like lett å overskue hvilke krefter som virker inn på vår vilje eller evne til å gjøre bruk av teknologi, men sammen med vår innovasjonsevne, vil kulturelle, politiske, økonomiske og markedsmessige faktorer påvirke den teknologiske utviklingen og hvordan vi kommer til å ta teknologien i bruk.

I dette kapittelet tar vi for oss noen av de sentrale teknologiene som er under utvikling. Vi vil imidlertid understreke at de teknologiske trendene vi presenterer har mange andre aspekter knyttet til seg enn de vi nevner. Vår fremstilling avgrenser seg til de aspektene ved disse teknologiene og trendene som utfordrer personvernet. Dette betyr ikke nødvendigvis at disse teknologiene og trendene representerer en særlig trussel mot personvernet, eller at de utfordringene vi peker på ikke vil la seg møte på en måte som ivaretar personvernet i tilstrekkelig grad. Vi har i fremstillingen nedenfor unnlatt å drøfte «for» eller «i mot» disse teknologiene, eller å si noe om sannsynligheten for at de utfordringene i forhold til personvernet vi peker på, vil materialisere seg.

9.1 Nanoteknologi

Et av de områdene der det sannsynligvis kommer til å skje mye på teknologisiden i årene som kommer, er såkalt «nanoteknologi». Nanoteknologi dreier seg om å kontrollere fysisk materie i svært liten skala (opp til ca. 100 nanometer). Det vil si fysisk materie på atom- eller molekylnivå.

Det spesielle med nanoteknologi er at den gir mulighet for integrasjon av informasjonsteknologi, molekylærbiologi og medisin til nye anvendelser. Av praktiske anvendelser tenker man seg klær som tilpasser seg miljøet, byggematerialer og nanomaskiner med regelbaserte sensorer, og ikke minst sensorer og maskiner som bygges inn i kroppen.

Slike sensorer/maskiner kan også settes opp for å utføre regelbaserte oppgaver, som automatisk registrering av for eksempel alkoholinntak hos yrkessjåfører, eller automatisk medisinering av folk under tvungent psykisk helsevern.

Nanoteknologien danner på mange måter en bro mellom den fysiske verden og den virtuelle verden, slik at disse går mer og mer over i hverandre.

Nanoteknologien har et enormt potensiale, men fordi den åpner opp for sensor- og kontrollteknologi på helt nye områder, inklusive inne i menneskekroppen, gir den også nye utfordringer for personvernet.

9.2 Kommunikasjonsteknologi

Utviklingen innen kommunikasjonsteknologi de siste årene har vært formidabel. Denne utviklingen vil fortsette, basert på videre utbygging og oppgradering av nasjonal telekommunikasjonsinfrastruktur og videre utbygging av Internett på faste linjer og trådløse nett.

Utbredelsen av slike nett, det område de dekker, og deres kapasitet og hastighet, vil øke. Både bruk av fiberbaserte nett, bakkenære trådløse samband og satellitt-teknologi vil øke. Flere deler av verden vil få tilgang til Internett. Dette gir nye muligheter for internasjonal utveksling av informasjon med de fordeler og ulemper som fraværet av nasjonale grenser for informasjonsutveksling innebærer. Globaliseringen og samarbeidet over landegrensene fører til både økt båndbredde på

optiske fibre, radio- og satellittbasert elektronisk kommunikasjon, og følgelig vil stadig flere, fra geografisk spredte familiegrupper til multinasjonale firmaer og verdensomspennende organisasjoner ta dette i bruk til intern kommunikasjon

I forholdet til brukerne har vi fått en utvikling med overgang fra bruk av faste linjer (kobbertråd og optiske fiberkabler) til trådløse samband (radiolinjer) og fra bruk av fasttelefon til bruk av IP-telefon og mulitimediatjenester. De trådløse nettene vil dominere hva angår offentlig aksess og aksess internt i bedrifters kontorlandskap.

Bruk av digital teknologi på alle typer media gjør det mulig å håndtere data, lyd og bilder integrert i produkter, i kommunikasjonsnettet og i datamaskinene. Dette har medført at tele-, data- og mediebransjene smelter sammen og visker ut grensene mellom kringkasting (radio og fjernsyn), tele- og informasjonsteknologi. De teknologiske løsningene for å gjøre alt digitalt, gjøres tilgjengelig for et massemarked, drevet fram av et politisk og kommersielt ønske om å fase ut kostbare analoge tjenester.

Globalisering av informasjonsutveksling og konvergens mellom ulike media, vil innebære en rekke utfordringer som vi vil drøfte nærmere i kapittel 13, om media og personvern.

9.3 Integrerte dataprosessorer i produkter

Den sentrale enheten i datamaskiner er prosessoren (CPU). Dette er enheten som kan programmeres og dermed settes i stand til å utføre alle typer logiske og matematiske operasjoner. Prosessoren har gjennomgått en rivende utvikling mht. pris/ytelse. Teknologiutviklingen har over flere år gitt en dobling av ytelse/pris hvert annet år. Dette betyr at etter om lag 15 år med en slik utviklingstakt, vil vi kunne ha tilgjengelig prosessorer med hundre ganger den ytelsen som tilbys i dagens marked, til samme pris som i dag.

Bare en beskjeden del av prosessorene som produseres, finner veien inn i det vi tradisjonelt betegner som en datamaskin. Størstedelen inngår som styringsenheter i alt fra leketøy og husholdningsartikler til biler og andre avanserte tekniske industriprodukter. I årene som kommer vil stadig flere produkter ha innebygde elektroniske komponenter med prosessorkraft og mulighet for datalagring (for analyse, logging og for sporbarhet).

Slike integrerterte dataprosessorer vil i økende grad bli tatt i bruk til registrering av data. Dette er noe man ser innen fremtidens transportmidler. Her vil det finnes mange komponenter som kan analysere, aksjonere, lagre og sende elektronisk informasjon. Vi kan oppleve at det meste vi kjøper og bruker av gjenstander i fremtiden vil inneholde en elektronisk brikke som registrerer ulike aspekter ved vår bruk av gjenstanden, og som det vil være mulig å avlese ved service, reklamasjoner, tvist med (skatte)myndighetene og lignende. Selskapet som har laget gjenstanden kan også tenkes å være interessert i slik informasjon for å drive med markedsanalyse, og for å skaffe seg mer kunnskap om sine kunder

Det at dataprosessorer og kommunikasjonsteknologi (jf. forrige punkt) snart vil finnes «overalt» kan føre til at de ulike produktene som har innebygd prosessorkraft vil begynne å «ringe hjem» og rapportere om hva brukeren foretar seg med produktet (Garfinkel 2000).

Antikollisjonssystemer i bilene er allerede innført og sørger for å redusere antall ulykker. Det finnes systemer (for eksempel EUs *eCall*) som automatisk kan registrere hvor ulykken har skjedd ved hjelp av det installerte satellittnavigasjonssystemet (GPS), ringer politi og verksted og eventuelt tilkaller ambulanse, registrerer skadeomfanget etc. Et slikt system kan også sørge for automatisk innkreving av veiavgifter og bompenger (uten bom). Og det kan produsere en logg som viser hvor bilen til enhver tid har befunnet seg og kan for eksempel stille denne informasjonen til rådighet for politiet, arbeidsgiver, ektefelle eller skattevesenet.

Det er også mulig, dersom man ønsker det, å plassere sensorer langs veien for å kommunisere med bilens styringssystemer, som sørger for at bilen ikke kjører fortere enn tillatte fartsgrense. Det store antallet bilulykker som skyldes at sjåføren er trøtt eller påvirket av rusmidler, gjør at kjøretøy i fremtiden kan bli utstyrt med et system som tvinger en trett eller beruset sjåfør til å parkere bilen ved at den nekter å starte.

Man kan komme til å se utviklingen bl.a. i bruk i avanserte alarmsystemer som automatisk varsler i spesielle ulykkestilfeller. Eller man kan se det i systemer for geografiske lokalisering, for eksempel ved at det vil bli vanlig å bære med seg en GPS-mottaker, gjerne integrert med mobiltelefonen eller armbåndsuret. I USA foreligger det forslag om å gjøre en GPS-mottaker til en obligatorisk komponent i en mobiltelefon, slik at det kan logges hvorfra oppringninger gjøres. Begrunnelsen for dette er bærerens sikkerhet. Et trykk på alarmknappen er tilstrekkelig for å varsle om posi-

sjon, eller den kan programmeres til periodisk å sende meldinger automatisk som gir posisjon, samt data fra en sensor for kroppstemperatur, hjertefrekvens, etc.

I USA har senator Ernest «Fritz» Hollings fra South Carolina foreslått en egen lov (*Security Systems Standards and Certification Act)* som vil gjøre en slik dataprosessor obligatorisk i *all* konsumentelektronikk som produseres eller omsettes i USA (Hannemyr 2005, s. 113). Så langt uten å få gjennomslag for dette.

9.4 Radiofrekvensidentifikasjon

Radiofrekvensidentifikasjon (RFID) er en metode for å lagre og hente data ved hjelp av små elektroniske enheter som kan avleses i form av radiosignaler. En RFID-brikke er svært rimelig å fremstille. Den kan identifiseres og spores trådløst.

RFID-brikker kan de nærmeste årene få en rekke nye anvendelsesområder ved at de blir en integrert del av de fleste produkter vi kjøper, enten det er hvitevarer, biler, offentlig transport, elektronisk utstyr, mat, sko, klær, helse, ID-kort, verdipapirer eller som implantater på dyr og mennesker.

Et argument for bruken av RFID er at man, ved å gjøre produkter og mennesker identifiserbare og sporbare, oppnår bedre livskvalitet og større effektivitet for næringsliv, offentlig virksomhet og kundebehandling. Et argument mot slik bruk er at brikkene legger til rette for kontinuerlig identifisering og sporing, og at dette truer privatlivet og personvernet.

For eksempel selger skoprodusenten Nike et produkt (*Nike+iPod Sport Kit*) der en slik brikke er plassert i en joggesko. Formålet med brikken er å gi brukeren økt helse og velvære ved å støtte opp om personlige treningsaktiviteter. Brikken sender ut radiosignaler som fanges opp av en medfølgende bærbar elektronisk enhet (*iPod*). Denne analyserer signalene, og gir på grunnlag av disse brukeren informasjon om løpt distanse, hastighet, treningsintensitet og lignende. Man kan imidlertid også tenke seg at brikken i skoen avleses trådløst av andre. RFID-brikken kan altså også benyttes til å spore den personen som bruker slike sko.

I USA er det søkt om patent (EP20070252636) på et system for å sikre at ansatte i restauranter og helseinstitusjoner ivaretar sin håndhygiene ved at en RFID-brikke den ansatte bærer på seg sporer den ansattes bevegelser. Systemet kan registrere når den ansatte benytter toalettet, når han eller hun vasker hendene, og når den ansatte arbeider med mat, steller pasienter, etc. Systemet er derfor i stand til å oppdage det dersom den ansatte etter et toalettbesøk, for eksempel, rører mat uten først å ha vasket hendene.

Nedenfor gis skjematisk eksempler på flere bruksområder:

- En RFID-brikke kan åpne låser i hus og bygninger, fungere som elektronisk billett på t-bane, tog og buss, eller foreta transaksjoner i butikker på bensinstasjonen etc.
- Fremtidens klær kan ha innebygde RFID-brikker som også virker etter en vask i vaskemaskin. De kan spore barn på skoler og i barnehager. I USA og Storbritannia bruker enkelte skoler slike brikker i klærne for å gi informasjon om når barna kommer/forlater skolen og tar skolebussen.
- RFID-brikker bygges inn i alle biler for å kunne finne bilen hvis den blir stjålet. Det er mulig å overvåke bilens geografiske posisjon døgnet rundt, hvilket også kan gi innsikt i andre forhold som f.eks. fysisk tilstedeværelse i jobb og familierelasjoner etc.
- Ved bestilling av reise kan du motta en elektronisk billett vedlagt en RFID-brikke som festes på bagasjen. Brikken gir flyselskapet full kontroll med din bagasje i forhold til reisested.
- Elektroniske RFID-brikker kan integreres i verdipapirer og fakturaer, slik at regninger og transaksjoner kan spores i forhold til bruk. Finansinstitusjoner kan telle penger på en raskere og mer effektiv måte, og illegale og legale transaksjoner vha. kontanter kan spores.
- Offentlig trafikkontroll kan gjennomføres ved at RFID-brikker festes på biler. Langs veien kan det settes opp skannere som kontrollerer fart, avstand og bevegelser. Basert på denne informasjonen ilegges bøter, bompengeavgifter og andre avgifter som sendes til din postadresse eller automatisk belastes din konto.
- Butikkene kan feste RFID-brikker på alle typer varer. Kundene kan ta de varene de ønsker og spasere ut av butikken. Betalingen skjer automatisk ved belastning av kundens konto. Samtidig blir butikkens varebeholdning automatisk oppdatert. En slik løsning gir imidlertid butikken, om den ønsker det, full oversikt over ditt forbruksmønster.
- En RFID-brikke kan plasseres som implantat under huden. Den kan lagre medisinske data, gi personlig identitet for både dyr og mennes-

ker, kontrollere tilgang til fysiske områder og spores ved forsvinning eller kidnapping.

En av de mest utbredte standardene for RFID-brikker (ISO 14443), gjør at brikken kan identifiseres opp til ca. 11 cm. Men det finnes også standarder som tillater identifisering på langt større avstander, opp til flere hundre meter.

Både pass og nasjonale ID-kort (i de land som har slike) er i ferd med å bli basert på RFID-teknologi. Disse inneholder gjerne elektronisk signatur, navn, adresse og foto, samt biometriske data som fingeravtrykk eller iris-data. Hensikten er å ha et kort eller pass som gir entydig identifisering av et individ. Et slik ID-kort kan tilrettelegges for ymse gjøremål, inkludert tilgang til tjenester fra offentlig sektor og næringslivet.

Motstanderne av slike pass og ID-kort mener dataene på kortet og de databaser som gir aksess fra kortet, ikke er beskyttet godt nok for misbruk og manipulering. Det er påvist at det er mulig å kopiere et slikt kort trådløst mens det befinner seg i eierens lomme (Daily Mail 2007).

Det finnes i dag elektroniske RFID-brikker på størrelse med et riskorn. Dyr kan utstyres med slike brikker ved at de opereres inn under huden (f.eks. i øret), og denne praksisen er forholdsvis utbredt. Det samme kan selvsagt også gjøres med mennesker.

Selskapet *Verichip* har siden 2007 eksperimentert med RFID-implantater i et system laget for å overvåke Alzheimer-pasienter (RFIDjournal 2007). En slik brikke kan også opereres inn i kroppen på andre personer man ønsker å følge bevegelsesmønsteret til. Ved å utstyre dem med slike brikker, kan man følge dem inne i bygninger, og eventuelt også utenfor, dersom man bygger ut sensornettverket. Selskapet *CityWatcher* i USA benytter allerede slike implantater til å spore hvor ansatte befinner seg (WorldNetDaily.com 2006).

Ekteparet Michael ved University of Wollongong har foreslått begrepet «überveillance» som betegnelse på en sensorbasert overvåkning som er konstant, og som invaderer menneskekroppen (Michael og Michael 2007):

> "Überveillance is an *above* and *beyond*, an *exaggerated*, an omnipresent 24/7 electronic surveillance. It is a surveillance that is not only "always on» but "always with you" (it is *ubiquitous*) because the technology that facilitates it, in its ultimate implementation, is embedded within the human body. The problem with this kind of bodily invasive surveillance is that *omnipresence* in the 'material' world will not always equate with *omniscience*, hence the real concern for misinformation, misinterpretation, and information manipulation."

9.5 Elektroniske brikker og kort

Elektroniske brikker og kort har vunnet innpass på en rekke områder. Dette er produkter som kan inneholde en identifikasjon og mindre mengder med assosierte data. Det kan også inneholde en liten dataprosessor som kan være i stand til å gjøre enkle beregninger (f.eks. smart-kort). Slike brikker og kort etterlater seg elektronisk spor i én eller flere databaser hver gang de blir benyttet. Dette er nyttig informasjon for forretningsvirksomhet, men dataene kan også være av interesse for politiet i forbindelse med etterforskning av kriminalsaker generelt. Sporene identifiserer brukeren, tidspunktet for bruken og identiteten til eventuelle mottakere av meldingen eller transaksjonen.

De fleste har ett eller flere slike kort i sin lommebok. Bankene og kredittselskapene var tidlig ute. De har senere blitt fulgt opp av bedrifter og handelskjeder som benytter kortet som et elektronisk identitets- og kredittkort (oljeselskaper, butikk-kjeder, hotellkjeder, flyselskaper, etc.).

9.6 Sensorteknologi

Det foregår en betydelig utvikling innenfor området sensorteknologi. Dette innbefatter utstyr som kan registrere og formidle måledata som enkeltmålinger eller kontinuerlige målinger. Produkter på dette området kjenner vi fra f.eks. radar- og laser-utstyr for måling av hastigheter, elektronisk utstyr for måling av alkoholkonsentrasjon, etc.

Fotokvaliteten har økt og prisen for bildekvalitet i et kamera har falt dramatisk de siste årene. De beste kameraene kan plukke ut en spesiell klokke eller en pakke sigaretter på en avstand av 500 meter med fulle farger og i mørke (ved å være følsomme for lys i det infrarøde området). Moderne kameraer er digitale, noe som betyr at bildene kan behandles med digital bildeforbedringsteknologi både i sanntid og ved senere analyse.

Avansert programvare på sensorer og digitale kameraer er en nyvinning som gjør det mulig bl.a. å oppdage tidlige tegn på røyk og/eller varmeutvikling før en brann blir utviklet, eller kan følge et bevegelig objekt ved at teknologien registrerer endringer i bildet som utløser alarm. En angitt person eller et bevegelig objekt (for eksempel en

bil) som fanges opp av et kamera, kan overvåkes selv gjennom en menneskemengde eller i en kjørebane. Teknologien sørger for at det automatisk kobles over fra et kamera til et annet i et overvåkningsnettverk med mange kameraer, og det iakttatte objektets bevegelser følges.

Et annet anvendelsesområde er veiovervåkning med automatisk gjenkjenning av bilers registreringsnummer ved bruk av infrarøde kameraer og mønstergjenkjenningsteknologi.

Når denne typen teknologi blir tilgjengelig kommersielt, vil det være et stort potensial for anvendelse i svært mange bransjer, også for privat beskyttelse, der man automatisk registrerer og følger opp mistenkelig adferd.

9.7 Biometri

Biometriske teknikker gjør det mulig å identifisere kjente personer blant flere tusen ansikter skannet fra et foto- eller videokamera. En benytter da digital teknologi for mønster- og ansiktsgjenkjenning. Biometri er begrepet som benyttes for et mangfold av måter å identifisere ulike deler av menneskekroppen. Fingeravtrykk er den mest vanlige biometriske metoden som fortsatt benyttes. Andre biometriske metoder er håndavtrykk, øyets irisoppbygning, blodforgrening, skriftmønster, kroppslukt, gangart, stemmemønster etc.

De mest aktuelle biometriske metodene som nå er på vei inn i anvendelse, er fingeravtrykk som brukes i adgangskontrollsystemer, geometri for menneskets ansikt, som brukes for å identifisere mennesker i en menneskemengde, samt sporing av biologisk materiale vha. menneskets unike sammensetning av gener i form av DNA-beskrivelse.

Programvare for ansiktsgjenkjenning integreres i overvåkningskameraer og gjør at de mest avanserte systemene kan gjenkjenne 500-1000 ansikter per sekund i en menneskemengde. Når systemet samtidig kan logge tid og sted for individer, gir det store muligheter for en automatisert overvåkning på private eller offentlige steder. De mest opplagte stedene dette kan anvendes på, er fotballkamper, konserter og parader hvor mange mennesker er samlet.

Den biometriske industrien vokser, blant annet som en følge av terrorfaren i Europa og USA. Mange flyplasser i USA og andre land har nå installert ansiktsgjenkjennende systemer med det formål å identifisere personer som er registrert som mistenkte for kriminalitet eller terror, automatisk.

Biometriske systemer er på full fart inn i banker og finansinstitusjoner for å avdekke bedrageri- og identitetstyveri-saker Andre typer næringsvirksomhet (spesielt i tjenesteyting, underholdning og spillbransjen) er i ferd med å ta i bruk slike systemer for å identifisere personer og brukere som mistenkes for falskneri, med den hensikt å få dem utestengt fra virksomheten. Ulike biometriske systemer tas også etter hvert i bruk for å sikre tilgang til datamaskiner innen både finans- og helseinstitusjoner. Stadig flere flyselskaper benytter elektronisk fingeravtrykk for å effektivisere adgangskontroll og billettservice.

Dersom slike biometriske systemer blir tatt i bruk på en omfattende måte, vil det bli mulig å kryssjekke og kombinere mange ulike typer databaser og registre for ulike formål. Det er mulig å tenke seg at næringslivet, banker og finanssektoren vil ha nytte av å bruke dette til finansielle overføringer. Det er også sannsynlig at offentlige myndigheter vil ha nytte av en samordning med utveksling av data mellom ulike databaser og registre for å effektivisere og øke servicenivået for sin virksomhet.

Som følge av mulighetene til blant annet automatisk å kunne identifisere uønskede individer som ligger i ansikts-, gangarts-, og mønstergjenkjenning, vil nytteverdien av kameraovervåkningssystemer øke. Allerede i dag er sosial ekskludering en vanlig anvendelse av overvåkningskameraer (Lomell 2005, Lomell 2007). Dersom dette kan automatiseres vil vi trolig se en økning i bruken av kameraovervåkning, både i offentlig og privat sektor.

En viktig trend når det gjelder kameraovervåkning er at det nå utvikles videobrikker med svært høy oppløsning til digitalkameraer for konsumentmarkedet. Dette gjør at prisen på slike sensorer faller dramatisk. Med høy oppløsning på bildebrikken kan også slike rimelige videokameraer ta i bruk programvare for ansikts-, gangarts-, og mønstergjenkjenning.

Slike systemer kan ha mange gode formål, men konsekvensene kan være ubehagelige hvis det oppstår feilsituasjoner. Det er nokså klart at mønster- og ansiktsgjenkjenningssystemer bare fungerer optimalt når systemet er kalibrert og har anvendt riktig digitale metode. Høye feilrater kan imidlertid oppstå. Hvis uskyldige mennesker blir uriktig identifisert som kriminelle og dette skyldes høye feilrater i teknologien, vil dette være uheldig og en uakseptabel bruk.

9.8 Trådløs kommunikasjon og lokaliseringssporing

Industrien som utvikler produkter og tjenester for det trådløse datakommunikasjonsmarked er i rask utvikling. Digitale mobiltelefoner blir mindre, billigere og byr på mer prosessorkraft. Mobiltelefonbrukere vil kunne skrive dokumenter, slå opp i sin avtalebok, få veianvisning på kart, høre på radio, lytte på musikk eller video, sende og motta elektronisk post/meldinger, låse opp dører, betale for varer, og surfe på Internett. Mobiltelefonen kan bli en håndholdt personlig datamaskin som også gir mulighet til å føre samtaler over telenettet eller mobilt Internett.

Mobiltelefoner kan også utstyres med et geografisk posisjoneringssystem med kartverk for nøyaktig stedsangivelser. Nødtjenester i USA argumenter for å gjøre dette til en obligatorisk funksjon i alle mobiltelefoner, slik at nødoppkall kan spores mer presist.

Informasjonsindustrien er i ferd med å lage en rekke nye brukertjenester som tar utgangspunkt i merfunksjonaliteteten som er i ferd med å komme på plass i mobiltelefoner og andre mobile enheter.

Man kan se for seg at mobiltelefonen du har med deg overalt, gir deg varsling om at du befinner deg i et område med for eksempel ulike typer butikker, restauranter, bensinstasjoner eller hva som helst, som du legger inn i din profil som interessant for deg. Hvis du reiser gjennom et tettsted, kan det gis et varsel i form av en stemme eller en melding om at du er nær en restaurant eller bensinstasjon.

Ulempene med et slikt system er at mobiltelefonen fungerer som en sporingsenhet. Det vil da være mulig for både offentlige myndigheter og private med egnet utstyr, å finne ut hvor du er med forholdsvis stor nøyaktighet, både i sanntid og i ettertid gjennom lokasjonsdata som er lagret hos offentlige telekommunikasjonstilbydere. Nye lovbestemmelser, som EUs datalagringsdirektiv, sikrer at lokasjonsdata blir lagret i lang tid etter at de ble registrert. Det å reise fritt og anonymt vil være vanskelig dersom man bærer med seg en mobiltelefon.

9.9 Internettavlytting

Internett brukes av mange til mange typer oppgaver som innholder kritiske data og personlig informasjon. Avlyttingsteknologien knyttet til nettet er i enorm utvikling både i forhold til ny teknologi og i forhold til metodikk. Det er derfor, både for samfunnet og det enkelte menneske, en utfordring at moderne avlyttingsteknologi gir mulighet for avlytting av alle type data som utveksles eller overføres på Internett, i noen tilfeller hvor som helst i verden (Hannemyr 2008a), med metoder som den vanlige bruker i liten grad vet om, eller kan sikre seg mot.

Utviklingen innenfor kryptografi har gjort det mulig for den enkelte å sikre sine data bedre mot avlytting, men samtidig har langt flere fått tilgang til avlyttingsteknologi. Tidligere var det i all hovedsak politiet og militære organisasjoner som lyttet. Nå er avansert utstyr for avlytting til salgs i butikker som retter seg mot konsumentmarkedet. Muligheten til å bli avlyttet har økt og vil øke som følge av at næringsvirksomhet, informasjonsindustri og privatpersoner som bruker åpne datanett som en hovedarena for fritidsaktivitet, arbeide og tjenesteyting.

Teknologi og metodikk for avlytting kan omfatte:

- Utlevere kopi av IP-pakker i sanntid med innhold og trafikkdata i knutepunkter hos teleoperatører og internettilbydere.
- Skadelig programvare plassert i en datamaskin som avlytter aktivitet ved maskinen over nettet. Vanligvis avlyttes tastetrykk, men moderne personlige datamaskiner er som regel utstyrt med mikrofon og videokamera, og disse kan også aktiviseres av skadelig programvare.
- Såkalte «cookies» og «webbugs» som identifiserer spesifikke brukere og samler inn sporingsdata gjennom å koble usynlige referanser i e-post eller nettsider til annen informasjon.
- Private og offentlige WLAN systemer som gjennom en feil er gjort åpne, eller er så dårlig sikret mot avlytting at de lett kan avlyttes.

9.10 Digitalt fjernsyn

Digitaliseringen av fjernsynet har pågått over flere år. De analoge sendingene i Norge opphører i sin helhet i løpet av 2009. Innen få år er fjernsyn et digitalt medium over det meste av verden. Digitaliseringen medfører endringer i produksjon, distribusjon og konsum av innhold og innholdsrelaterte tjenester.

Med noen få unntak (f.eks. innringingsprogrammer og eksperimenter der seerne kan få vist

SMS-meldinger i rulletekst på skjermen) er den tradisjonelle fjernsynsteknologien i hovedsak enveis. Dette skiller tradisjonelt fjernsyn fra Internett som tilbyr interaktive toveistjenester for en rekke ulike formål og behov.

Inntil nylig har både innhold, aktører, teknologi og verdiskapning for henholdsvis fjernsyn og Internett skjedd i gjensidig isolasjon. Dette er i ferd med å endre seg. For eksempel er videoinnhold i form av filmer, aktualitetsprogrammer og serier i ferd med å bli tilgjengelig via Internett. I samband med at såkalte *Settop-bokser* tas i bruk for digitalt fjernsyn muliggjøres interaktive tjenester og funksjoner som forutsetter toveis-kommunikasjon (Hannemyr 2002, s. 52). Denne utviklingen, som mange refererer til som konvergens mellom Internett og fjernsyn, vil endre roller og forretningsmodeller for alle aktørene i verdikjeden. Innholdsleverandører (som NRK, TV2, BBC), distributører (som ViaSat og Canal Digital), og nettverksoperatørene (Telenor, NextGenTel osv.). De tradisjonelle fjernsynsdistributørene tar vanligvis betalt av brukerne gjennom faste abonnementer. En ny type tjenesteleverandører på Internett (innholdsaggregatorer) har imidlertid demonstrert at det er mulig å tjene penger på modeller der man tilbyr attraktive tjenester og innhold gratis, ved at annonsører betaler for å være til stede der mange brukere samles (jf. YouTube, Facebook, Yahoo, Google, etc.), og ikke minst ved at annonsørene får tilgang til mer informasjon om brukerne enn det som er vanlig i samband med tradisjonell fjernsynsreklame.

Internett er – i motsetning til tradisjonelt kringkastet TV – velegnet til å følge individuell brukeradferd. Slik informasjon kan benyttes til å kartlegge individers og segmenters preferanser og kjøpsvillighet til ulike varer og tjenester, som i sin tur selges til annonsører i form av individrettet markedsføring. Denne type tjenesteyting vokser raskt, og er i sin natur grensekryssende og global. Felles internasjonal lovgivning mangler. Tjenestene er ofte basert på passivt samtykke (ved å bruke tjenesten samtykker man til at tjenesteyter registrerer opplysninger om forbrukeradferd). Det er ikke alle som er oppmerksom på hva et slikt passivt samtykke innebærer.

Denne typen individrettet markedsføring har vist seg å være svært effektiv. Det er derfor fare for at kjøpsadferden endres – ikke som følge av personlige valg – men fordi innsamlet og bearbeidet adferdsinformasjon kan brukes til å manipulere det enkeltes individs kjøpeadferd og preferanser.

9.11 DNA-profilering

Hvert menneske bærer en biologisk kode som kalles DNA. Denne koden brukes blant annet for å identifisere personer og kan benyttes som bevis i kriminalsaker.

I Europa etableres nasjonale DNA databaser der personinformasjon kan utveksles ved saker som har internasjonal forankring. Kriteriene for å ta DNA-prøver og få dem utlevert er noe forskjellig i ulike land. Siden DNA-koden kan gi medisinsk informasjon om arvelighet og sykdom, er dette svært sensitiv informasjon om personer som må håndteres i henhold til gode etiske og rettslige prinsipper. Selv om hele DNA-koden ikke registreres, slik at det ikke er mulig å hente ut medisinsk informasjon, vil opplysningene være sensitive fordi registrering i DNA-registeret (i Norge) samtidig gir informasjon om at du er domfelt for et straffbart forhold som kan medføre fengselsstraff.

9.11.1 DNA-registeret i Norge

I Norge har man hatt et DNA-register til bruk i etterforskning og straffesaker siden 1995. Registret har hjemmel i straffeprosessloven § 160a. Nærmere regler for registrering og bruk finnes i påtaleinstruksen kapittel 11a.

Opprinnelig var adgangen til registrering begrenset til alvorlige straffbare forhold, som allmennfarlige forbrytelser, seksualforbrytelser og ran. I september 2008 ble registreringsadgangen utvidet. Nå kan alle som domfelles for en handling som kan medfører frihetsstraff registreres i DNA-registeret. I tillegg har man etablert et etterforskningsregister der man midlertidig registrerer DNA-profiler fra personer som med skjellig grunn mistenkes for en straffbar handling som kan medføre frihetsstraff. Midlertidige profiler slettes ved rettskraftig henleggelse eller frifinnelse. Registeret har også et sporregister, som inneholder DNA-profiler med tilknytning til uoppklarte straffesaker fra personer med ukjent identitet.

Den utvidede adgangen til å registrere også mindre alvorlig kriminalitet er begrunnet i et ønske om å identifisere lovbrytere så tidlig som mulig. Man tenker seg at økt registrering vil gi vesentlig økning i oppklaringsprosenten, noe som en antar igjen vil redusere kriminaliteten.

DNA-registrering har en side mot personvernet. Blant annet kan det biologiske materialet som danner grunnlaget for registreringen gi opphav til

opplysninger om blant annet helseforhold. Biologisk materiale som har vært analysegrunnlag for DNA-profiler skal imidlertid destrueres så snart registrering av profilen har funnet sted, jf. påtaleinstruksen § 11a-8. Dette forutsetter at det utarbeides gode faktiske rutiner som sørger for at lovens krav etterleves på dette punktet. Når det gjelder opplysninger i identitetsdelen, slettes det ingen opplysninger her før etter at den registrerte er død (og ev. ved frifinnelse etter gjenopptakelse). Flere har påpekt at mangelen på differensierte sletteregler er en utfordring for personvernet.

Kapittel 10
Personvernfremmende teknologier

I personvernkretser har det vært debatt om hvilke teknologier som faller innenfor begrepet personvernfremmende teknologier eller PETs (engelsk: *privacy enhancing tehnologies*). Mange som arbeider med dette fagfeltet ønsker å avgrense PETs til kun å dreie seg om teknologier for anonymisering, pseudonymisering og identitetsforvaltning.

For eksempel hevdes det at teknologier rettet inn mot personlig datasikkerhet ikke hører inn under PETs.

Videre diskuteres det om kryptografi faller inn under PETs. Benyttes kryptografi som ledd i en anonymiserings- eller pseudonymiseringsprosess, teller den med. Er det snakk om innholdskryptering for å sikre mot innsyn i opplysninger som kommuniseres eller som er lagret, vil dette være et rent informasjonssikkerhetstiltak. Kryptering har da som siktemål å verne opplysningene fra uautorisert innsyn (konfidensialitet) eller endring (integritet), og angår ikke identitet og muligheten for identifisering.

Denne debatten har primært akademisk interesse og Personvernkommisjonen vil under overskriften «personvernfremmende teknologier» både ta for seg teknologier som ikke spesifikt handler om identitetsforvaltning og teknologier som gjør dette. De første tar vi for oss i et avsnitt som summarisk drøfter ulike enkle teknologier som vi mener kan fremme personvernet. I det andre avsnittet tar vi for oss personvernfremmende teknologi som er knyttet til identitetsforvaltning.

10.1 Enkle personvernfremmende teknologier

10.1.1 Personlig datasikkerhet

Det er ingen tvil om at en rekke av de utfordringene personvernet står overfor, og som vi nevnte en del eksempler på i kapittel 9, kan møtes med teknologi som er konstruert for å løse ulike integritets- og sikkerhetsutfordringer.

Eksempler på dette er kryptering, brannmurer, antivirus, antispyware, spamfilter, egne modi i nettleseren som sletter spor og «cookies», osv.

Det som her bør sies, er at dette i første rekke dreier seg om ulike tekniske tiltak, som gjerne er knyttet til den enkelte brukers personlige utstyr. Personvernkommisjonen mener at verktøy for å ivareta personlig datasikkerhet og integriteten til eget datautstyr er viktig for den enkeltes personvern og personopplysningsvern. Vi har imidlertid ikke mulighet til å gå dypt ned i denne materien, men nøyer oss med å bemerke at kunnskap om riktig bruk av slik teknologi bør styrkes gjennom informasjon og opplæring.

10.1.2 Anonyme alternativer

Et klassisk eksempel på overvåkningsteknologi er en fotoboks som avfotograferer alle som kjører over fartsgrensen. Det er ikke spesielt kontroversielt, fordi den er målrettet mot kriminalitetsbekjempelse, og fordi man kan velge å unngå å bli fotografert (ved å holde fartsgrensen).

Men et slikt kamera genererer overskuddsinformasjon. Blir du fotografert, viser den hvor du var på et bestemt tidspunkt, hvem du ev. var sammen med og hva slags last du hadde i bilen og på taket.

Og dersom formålet med en slik boks er å sørge for at folk holder fartsgrensen, kan dette løses på en alternativ måte på veistrekninger som egner seg for lysregulering (dvs. i urbane områder). For eksempel kan trafikkflyten reguleres med trafikklys. Følere i veibanen kan måle hvilken hastighet bilene har. Disse dataene brukes til å styre lyskryssene, uten at personopplysninger registreres eller lages. Styringen kan konstrueres slik at biler som holder lovlig hastighet skal få grønn bølge, mens biler med for høy fart forsinkes av at de får rødt lys i alle kryss. Dermed «belønnes» førerne som holder fartsgrensen, uten at noen form for personopplysninger registreres eller lagres.

Personvernkommisjonen mener at det i alt for mange tilfeller iverksettes overvåkning når formå-

let ved overvåkningen kunne oppnås minst like godt og effektivt ved alternativ anvendelse av teknologi. Som vi belyser gjennom eksemplet over kan det, i alle fall i noen situasjoner, oppnås like gode resultater ved alternativ anvendelse av teknologi. Kommisjonen vil derfor oppfordre til at man, når man finner grunn til å iverksette overvåkning, utreder om man kan oppnå det samme på en alternativ måte.

10.1.3 Tilbaketrekking som gjør anonymitet mulig

Mange av teknologiene som griper inn i personvernet tolereres eller aksepteres av mange fordi de bidrar til å gjøre hverdagen enklere og mer bekvemme for brukerne.

Men det er viktig at designet i så fall inneholder en mulighet til såkalt tilbaketrekking (engelsk: *opt-out*) for kunder eller brukere som prioriterer personvern fremfor bekvemmelighet.

Dersom det for eksempel legges opp til bruk av RFID-brikker for debitering av kollektivreiser eller passering av bomringer, bør det legges til rette for at det også et anonymt tilbud i form av forhåndsbetalt anonymt «klippekort» eller lignende. Dette drøftes grundigere i kapittel 17 om kommunikasjonssektoren.

10.1.4 Søkemotorimmunisering

Fra nyhetsbildet kjenner vi også til at menneskelige feil har ført til at dokumenter som kan knyttes til navngitte personer og som innholder sensitive personopplysninger, har blitt lagt på nett. Slike dokumenter fanges så opp av søkemotorer, som Google, og vil bli funnet så snart noen gjør et nettsøk på det eller på navn som finnes i dokumentet.

Det er her viktig å merke seg at selv om det selvsagt er skadelig for personvernet at slike feil skjer, så øker konsekvensene av slike feil dramatisk i det øyeblikket dokumentene fanges opp av søkemotorene. Det skyldes to omstendigheter. For det første at dokumentet blir finnbart med søk på det relevante egennavnet. For det andre at det ikke lenger er tilstrekkelig å slette dokumentet ved kilden for å slette det fra nettet. Søkemotoren har nemlig tatt vare på en kopi i sin såkalte *cache*, og der vil det leve i opp til seks måneder, med mindre det tas eksplisitte grep for å få det slettet.

Søkemotorimmunisering er et enkelt grep som ethvert nettsted kan ta for å forhindre at søkemotorer på nettet automatisk indekserer og lagrer kopier av innhold. Vi mener at alle organisasjoner som håndterer sensitive personopplysninger rent rutinemessig bør immunisere sine nettsteder eller deler av disse mot søkemotorer.

10.1.5 Kryptering

Kryptering vil si å skjule informasjon ved å bearbeide de dataene der informasjonen er representert på en slik måte at bare de som er autorisert til å dekryptere dataene har mulighet til å få tilgang til informasjonen.

Fra nyhetsbildet er vi kjent med at personopplysninger kommer på avveie i en rekke ulike sammenhenger. Det kan være CD-plater med slike opplysninger som forsvinner i posten, e-post som feiladresseres, minnepinner som mistes på bussen, mobiltelefoner som glemmes igjen i barer, bærbare datamaskiner som blir stjålet, eller stasjonære datamaskiner som selges brukt – mens personopplysninger fremdeles er lagret på det aktuelle medium.

Alle som håndterer et medium der det finnes personopplysninger bør utvise stor aktsomhet, slik at episoder som beskrevet ovenfor ikke inntreffer. Likevel vet vi at menneskelige feil skjer, og utvilsomt vil skje igjen. Det er en klar tendens til at bærbare enheter både blir mindre (og derfor enklere å miste) og kraftigere, og det er bare et tidsspørsmål før bærbare datamaskiner og mobiltelefoner smelter helt sammen.

I alle tilfellene vi kjenner fra mediene ville skaden for personvernet ved at slike gjenstander eller forsendelser kommer på avveie vært eliminert dersom man hadde sikret dataene tilstrekkelig med kryptering. (Dette betyr selvsagt ikke at kryptering løser alle problemer for personvernet, bare de spesifikke problemene som knytter seg til uautorisert innsyn når lagringsmedia med sensitive data faller i gale hender.)

Kryptering er en forholdsvis moden teknologi som er enkel å ta i bruk. Det meste av dagens utstyr, fra mobiltelefoner til minnepinner, kan settes opp med effektive systemer som automatisk krypterer alt som er lagres på dem. Også for elektronisk post finnes det kryptering som er enkel å bruke. Det som imidlertid mangler er bevissthet og kunnskap om hvordan man bruker kryptering. Det mangler også en fungerende infrastruktur for utveksling og autentisering av offentlige kryptografiske nøkler (PKI – *public key infrastructure*).

Vi mener at å ruste opp brukermiljøer som håndterer personopplysninger i riktig og effektiv bruk av kryptering er et tiltak som bør settes i

verk, og at ikke minst PKI snarest bør på plass (dette er for så vidt arbeid som pågår, men det har tatt veldig mye lenger tid enn forventet).

Samtidig ønsker kommisjonen å bemerke at kryptering ikke bør betraktes som et alternativ til andre personvernfremmende tiltak.

10.2 Teknologier for identitetsforvaltning

Litteraturen om personvernfremmende teknologier, eller PETs (fra engelsk: *Privacy Enhancing Technologies*) dreier seg om tekniske og organisatoriske tiltak som tar sikte på å begrense andres mulighet til identifisere den enkelte.

Begrepet PETs kan føres tilbake til en rapport som datatilsynsmyndighetene i Ontario (Canada) og Nederland la fram i 1995. Rapporten «Privacy-enhancing technologies: the path to anonymity» (Hes og Borking 1995) ble første gang presentert på den 17. internasjonale datatilsynsmyndighetskonferansen i København samme år. Rapporten pekte på at det er mulig å konstruere informasjonssystemer slik at datasubjektets identitet holdes helt eller delvis skjult, uten at vesentlig funksjonalitet med hensyn til å følge datasubjekter over tid, går tapt. Dette var mulig ved å ta i bruk en pseudonymisert identifikator, «the identity protector». Kjernen i systemet var en koblingssentral hvor personidentifiserende identifikatorer (som for eksempel fødselsnummer) ble gjort om til pseudonymer som ikke direkte kunne knyttes til noen identifiserbar person. Slike koblingssentraler mellom identifiserbare identifikatorer og pseudonymer kunne plasseres i informasjonssystemets ulike deler eller være under brukerens kontroll. Rapporten anviste hvordan slike koblinger kunne skje automatisk i systemet etter nærmere bestemte regler forvaltet av en uavhengig og tiltrodd pseudonymforvalter.

Selv om begrepet «personvernfremmende teknologier» og akronymet «PETs» er relativt kjent i miljøer som arbeider med personvernspørsmål, finnes det fremdeles ingen omforent definisjon. Kjernen i begrepet har imidlertid hele tiden vært dataminimalitet, nærmere bestemt i forhold til å begrense muligheten for å identifisere den opplysningene gjelder, jf. Herbert Burkerts definisjon:

> "The term privacy-enhancing technologies (PETs) refer to technical and organizational concepts that aim at protecting personal identity. (Burkert 1997)"

Fokuset på (mangel på) identitet kan forklares ved at personopplysningsvern bare er relevant dersom den som opplysningene gjelder kan identifiseres. Dette faktum gjenspeiles i personopplysningslovgivningen, som bare gjelder i den grad det behandles opplysninger om en identifiserbar person. Det tradisjonelle fokuset mht. PETs dreier seg følgelig om løsninger for anonymitet og pseudonymitet.

Personvernkommisjonen vil imidlertid peke på at denne typen teknologi også lar oss betrakte disse spørsmålene om identitet og identifiserbarhet under synsvinkelen *identitetsforvaltning*, og at dette gjør denne typen teknologi langt mer anvendelig.

Identitetsforvaltning tar utgangspunkt i individets ulike roller og hvordan identifisering og autentisering kan tilpasses disse rollene og relasjonene. Dette er et område med betydelige utfordringer, både når det gjelder teknologiutvikling, infrastruktur og regulering.

I Norge kjenner vi primært personvernfremmende teknologi fra et offentlig utvalg ledet av professor Erik Boe som utredet hvordan man kunne forene samfunnets behov for forskning på helseopplysinger med ivaretakelsen av den enkeltes personvern. Mens man tidligere hadde skilt mellom anonyme eller avidentifiserte opplysninger (som ga relativt begrensede muligheter for forskning) og fullt ut identifiserbare opplysninger (som medførte en ikke ubetydelig personvernrisiko), ble det i NOU 1993:22 (*Pseudonyme helseregistre*) foreslått en radikal endring i måten å organisere helseregistre på. I stedet for å lagre helseopplysinger med fødselsnummer, ble det foreslått at opplysningene skulle lagres under pseudonymer generert av en tiltrodd pseudonymforvalter. Tankegangen og prinsippet var det samme som i PETs-rapporten fra 1995: Ved å bytte ut personidentfiserbare identifikatorer med pseudonymer, kunne man oppnå samme funksjonalitet, samtidig som risikoen for personvernkrenkelser ble vesentlig redusert.

Dessverre ser det ut til at dette arbeidet verken er forstått eller tilfredsstillende fulgt opp (se for øvrig kapittel 16 om personvern og helse).

Vi viser forøvrig til vedlegg 4, der Thomas Olsen gjør grundigere rede for teknologier for identitetsforvaltning.

Kapittel 11
Forslag til tiltak

Personvernkommisjonen mener at ved introduksjon av ny teknologi i samfunnet bør som hovedregel teknologiens innvirkning på personvernet utredes på lik linje med teknologiens innvirkning på miljø og økonomi.

Personvernkommisjonen mener videre at det er viktig at samfunnet har fokus på teknologiutviklingen og fanger opp tendenser, både når det gjelder personvernfremmende teknologier og ny teknologi som kan true personvernet.

I den sammenhengen vil kommisjonen fremheve Datatilsynets faglige virksomhet (jf. kapittel 18) og det arbeidet som gjøres av Teknologirådet med å kartlegge og formidle teknologiutviklingen til politikere og publikum. Det er viktig at begge organers arbeid på dette området fortsetter, og at de har tilstrekkelig med ressurser til å ivareta dette viktige arbeidet.

Personvernkommisjonen mener det bør være en prioritert offentlig oppgave å ruste opp brukermiljøer som håndterer personopplysninger i riktig og effektiv bruk av kryptering. Tiltak på dette området bør snarest settes i verk.

Videre bør det pågående arbeidet med infrastruktur for distribusjon av offentlige kryptografiske nøkler (PKI) intensiveres.

Del IV
Særskilte områder kommisjonen har sett på

Kapittel 12
Innledning

I Personvernkommisjonens mandat er det fremhevet noen konkrete områder/sektorer hvor personvernutfordringene er mange og vanskelige. Kommisjonen ble derfor bedt om å ha særskilt fokus på spørsmål som gjaldt personvern og media, personvern for barn og unge, personvern i arbeidslivet, personvern i helsesektoren, samt personvern i samferdselssektoren. I dette kapittelet presenteres Personvernkommisjonens observasjoner og forslag til tiltak innenfor de ovennevnte områdene.

Kapittel 13
Personvern og media

Den delen av Personvernkommisjonens rapport som tar for seg personvern og media består av fem avsnitt. I avsnitt 13.1 presenteres en del sentrale begreper. I avsnitt 13.2 redegjør vi for hvordan personvern i mediene reguleres gjennom lover, forskrifter, internasjonale konvensjoner, rettspraksis, forvaltningspraksis, yrkesetiske retningslinjer, avtaler, samt gjennom allmennmoralen. I avsnitt 13.3 tar vi for oss ulike medietyper og redaksjonelle praksiser, samt hvilke utfordringer dagens mediemangfold skaper for personvernet. I avsnitt 13.4 presenteres ytterligere to områder som vedrører media og personvern, men som ikke henger sammen med medietyper og medieroller – nemlig offentliggjøring av skattelistene og elektronisk pliktavlevering. Til sist, i avsnitt 13.5, kommer vi med forslag til tiltak som kommisjonen mener vil styrke personvernet i forhold til mediene.

13.1 Sentrale begreper

For en definisjon av begrepene personvern og personopplysningsvern, se kapittel 4.1.5.

13.1.1 Forholdet mellom personvern og ytringsfrihet

Med ytringsfrihet menes friheten til å ha en hvilken som helst mening, til offentlig å formidle meninger, fakta og ideer, og til å motta disse.

Skal mediene fungere slik vi ønsker det i vårt demokrati er ytringsfriheten viktig. Dette er både fordi ytringsfriheten danner mye av medienes grunnlag, og fordi ytringsfriheten tjener bredere samfunnsmessige interesser, særlig interessen i å avdekke sannhet. I *On Liberty* begrunner John Stuart Mill (1806-73) ytringsfriheten med at det kun er når de riktige oppfatninger brytes mot de gale, at samfunnet kan nærme seg hva som faktisk er riktig (jf. også NOU 1999:27 «Ytringsfrihed bør finde Sted», utredning fra den norske Ytringsfrihetskommisjonen, s. 20).

Men noen ganger utfordrer mediene personvernet. Dette kan for eksempel skje når mediene formidler informasjon om en person som angår vedkommendes integritet, privatliv, ære eller personlige forhold. Personopplysningsvernet utfordres av mediene når personopplysninger samles inn, bearbeides og publiseres.

Når slike utfordringer oppstår, er det altså to viktige hensyn som blir stilt opp mot hverandre: personvernet og ytringsfriheten. Begge hensyn er viktige, både for enkeltindivider, grupper og samfunnet. Og begge har stor normativ tyngdekraft. Dette kommer til uttrykk i (og følger av) rettssystemet. Begge hensyn er nedfelt som grunnleggende rettigheter blant annet i Den europeiske menneskerettighetskonvensjonen (EMK).

Som vi kommer tilbake til i kapittel 13.2.1 er ingen av disse rettighetene absolutte. Retten til privatliv innebærer for eksempel ikke at offentlig myndighet er avskåret fra å gripe inn mot vold innen hjemmets fire vegger. Og ytringsfriheten er begrenset, for eksempel for rasistiske uttalelser.

Innledningsvis er det også viktig å påpeke at personvern og ytringsfrihet er likeverdige hensyn og rettigheter. Den ene har i utgangspunktet ikke normativ forrang over den andre.

Det er videre viktig å påpeke at ytringsfrihet og personvern ikke alltid er på kollisjonskurs med hverandre. Ivaretakelse av et personvern er i mange sammenhenger en forutsetning for ytringsfriheten, dvs. utøvelsen av frihetene til å samles, til å ytre seg og til å søke opplysninger, uten å behøve å frykte at slike aktiviteter vil bli lagt en til last.

13.1.2 Om begrepet massemedia

Massemedia (som vi ofte forkorter til bare «media») er midler for kommunikasjon som befinner seg utenfor den private sfære. Denis McQuail (professor emeritus i massekommunikasjon ved universitet i Amsterdam) definerer dem slik (McQuail 2000, s. 4):

> "The term 'mass media' is shorthand to describe means of communication that operate on a large scale, reaching and involving virtually everyone in society to a greater or lesser degree. It refers to a number of media that are now long-established and familiar, such as newspapers, magazines, film, radio, television and the phonograph (recorded music). It has an uncertain frontier with a number of new kinds of media that differ mainly in being more individual, diversified and interactive and of which the Internet is the leading example. "

Massemedienes arena er det offentlige rom. Den teknologiske utviklingen har de siste årene åpnet for nye muligheter for spredning av informasjon, men også åpnet opp for en rekke nye utfordringer, ikke minst i forhold til personvern.

Utviklingen innefor massemediene karakteriseres ofte med begrepet «konvergens». Begrepet er dannet av det latinske *con vergere*, som betyr «å løpe sammen, nærme seg hverandre». Med konvergens siktes det blant annet til at informasjons- og kommunikasjonsstrømmer som tidligere har eksistert innenfor relativt atskilte arenaer (eksempelvis aviser, bøker, fotografi, vinylplater, telefoni, televisjon, shopping, osv.) løper sammen på den måten at de blir distribuert over samme kanaler og nettverk. Dette skjer delvis på grunn av at disse informasjons- og kommunikasjonsstrømmene blir «digitale» (dvs. tuftet på digital koding og overføring av informasjon).

Men paradoksalt nok fører digitaliseringen også til *divergens*. De «nye» mediene er ofte langt mer komplekse og mangfoldige enn de «tradisjonelle» mediene, både når det gjelder sjanger, spredning, produksjon, fordeling av ansvar, roller og identitet. Dette mangfoldet er selvsagt en berikelse, men det skaper også utfordringer i forhold til personvern og personopplysningsvern. Dette kommer vi tilbake til i kapittel 13.3.

13.1.3 Om begrepene offentlighet og privatliv

Personvern handler blant annet om vern av den private sfære. Når det private blir offentlig er personvernet selvsagt under press. Men det er ikke bare personvernet som da blir satt under press; også kvaliteten på den «offentlige samtalen» står i fare for å bli forringet.

I utredningen fra Ytringsfrihetskommisjonen (NOU 1999:27, s. 28-29) står følgende:

> «Den private sfære […] er sfæren der man omgås med dem man kjenner som personer. Den er, og bør være, en frihetssfære i den forstand at den i omfattende grad er beskyttet mot reguleringer og inngrep fra det offentlige. […]
>
> Privatsfæren er, og bør være, en frihetssfære også i den forstand at den er beskyttet mot innsyn så vel fra det offentlige som fra offentligheten. Disse to friheter, mot inngrep og innsyn, er en forutsetning for dannelsesprosessen og identitetsutviklingen frem mot det myndige menneske. […] Man kan bare utvikles som menneske ved at man har et rom der man kan føle seg fri fra å måtte stå til ansvar for hva man gjør eller sier overfor ytre, ukjente kontrollører. Den offentlige samtale i et fritt samfunn har sitt utgangspunkt i slike fri og utvungne prosesser, den springer frem fra den beskyttede privatsfære. […]
>
> Tendensen til utvisking av skillet mellom den private og den offentlige sfære innebærer på den ene side en offentliggjøring av det private, og på den annen en privatisering av det offentlige. Det første henspiller på den skade utviskingen kan få for dannelsesprosessene i privatsfæren, slik som antydet ovenfor. Det annet henspiller på den skade utviskingen kan få for den offentlige kommunikasjonen. […] Dette er … skadelig ikke bare fordi det bryter med en rett til privatliv, men fordi den korrumperer den offentlige samtale slik at denne ikke kan fungere etter forutsetningen, men forfaller til sladder.»

Ytringsfriheten, slik den er nedfelt i Grunnloven § 100, legitimerer derfor ikke at mediene ubetinget kan trenge inn i den private sfære. Men mediene rapporterer ofte om hendelser som finner sted i den private sfære, eller om hendelser der den som er omtalt, er en privat (i motsetning til offentlig) person.

Enkelte personer befinner seg mer i offentlighetens søkelys enn andre. Politikere, kunstnere, idrettsstjerner, såkalte «kjendiser», og fremtredende embetspersoner omtales gjerne som «offentlige personer». Men også offentlige personer har krav på et privatliv.

Skjæringsflatene mellom en privat og offentlig sfære, og en privat og offentlig person kan illustreres med firefelts-skjemaet (figur 13.1) neste side (gjengitt etter innspill til Personvernkommisjonen fra presseforskeren Svein Brurås)

Privat sfære, privat person

Vi ser ofte i mediene eksempler på hvordan mange, og spesielt kjendiser, bevisst bruker opplysninger fra deler av sin private sfære for å få offent-

	Privat sfære	*Offentlig sfære*
Privat person	«Sjalusien ødela ekteskapet vårt» Hvordan skal mediene forholde seg til privatpersoner som *ønsker* oppmerksomhet om sitt privatliv?	«Mann skadet i bussulykke» Hvor nærgående kan ulykkes- og kriminaljournalistikk være uten å krenke privatlivet til de som er involvert?
Offentlig person	«Statssekretær havnet i fyllearresten» Også offentlige personer ruser seg, rammes av sykdom, inngår og bryter relasjoner, etc.	«Ministeren åpnet ny vei» Uproblematisk.

Figur 13.1

lig oppmerksomhet, eller for å oppnå andre ting. Mediene har også en egen interesse av å bruke slik informasjon. Når de samme personene ikke ønsker åpenhet om andre deler av sitt privatliv oppstår det lett konflikter med mediene. I samband med en rettssak om privatlivets fred spissformulerte daværende sjefredaktør i Se og Hør, Knut Haavik, denne konflikten på følgende måte «Når vi blir invitert til bryllupet, dekker vi også skilsmissen» (VG 1992). Retten var ikke enig i at fordi en person i en kontekst hadde gitt tilgang til sitt privatliv, så åpnet dette opp for at pressen hadde rett til å dekke andre sider ved privatlivet. Se og Hør tapte saken (RG 1995, s. 1145).

De nye tilbud som digitaliseringen har skapt, gir i tillegg den enkelte nye muligheter til selv å formidle deler av den private sfære ut i det offentlige rom. Det skjer gjennom såkalte nettsamfunn og gjennom privatpersoners egne kanaler av ulike slag, som blogger og fotoalbum. Mye av det materialet som legges ut kan være av privat karakter og ikke beregnet for offentlig innsyn. Det finnes mange eksempler på at legeerklæringer, flatfyll-fotografier, opptak med skjult mikrofon etc. er lagt ut på nett tilgjengelig for alle som måtte finne det. Mange er øyensynlig ikke bevisste på at når materiale er lagt ut på nett, så har man ikke lenger kontroll over spredningen eller bruken av det. Nettsamfunnet *patientslikeme.com*, som drives av en organisasjon som beskriver seg selv som ett «non-profit biotechnology laboratory» inviterer sine medlemmer til å laste opp diverse personopplysninger som detaljerte diagnoser, sykejournaler, personlig sykehistorie, og familiehistorie. Disse blir så gjort tilgjengelig for eksterne samarbeidspartnere, for eksempel forskningsinstitusjoner og legemiddelindustri, og publisert på Internett. Mange pasienter gjør dette. Noen av dem legger også ut fullt navn og bilde eller andre opplysninger som gjør dem identifiserbare. I hvilken grad skal *samfunnet* (gjennom rettsapparatet og forvaltningsorganer) kunne gripe inn og beskytte mennesker som selv legger ut egne sensitive personopplysninger mot seg selv?

Når et medium bretter ut forhold fra den private sfære på en måte som opplagt griper inn i integriteten til den omtalte, er da samtykke fra vedkommende en tilstrekkelig god grunn til å sette vedkommendes personvern til side? I hvor sterk grad plikter *mediene* å beskytte mennesker mot seg selv?

Hva om det er barn involvert? Juridisk sett har foreldre rett til å gi samtykke på vegne av mindreårige barn i de fleste anliggender. Men bør foreldre også ha rett til å krenke eller sette til side barnets personvern? Bør ansiktene sladdes når mediene publiserer pressebilder der barn er til stede i bilderuten?

Særlig problematisk blir det gjerne når en av partene i en barnevernssak eller barnefordelingstvist ønsker å bruke mediene til å fremme sin sak. Slike saker blir spesielt problematiske fordi det er barn som står i sentrum.

Erfaringene så langt viser at dette er et område som det er vanskelig å lage gode kjøreregler for. Hver sak må gjerne vurderes individuelt. Dette krever en spesiell aktsomhet fra alle parter og ikke minst mediene. En kritisk offentlig debatt rundt medienes rapportering fra privatlivet og større bevissthet omkring de etiske retningslinjer som angår rapportering fra den private sfære bør bidra til å styrke personvernet.

Privat sfære, offentlig person

Som vi utdyper i kapittel 13.2.2, der vi beskriver rettspraksis på området, er uttrykket «allmenn interesse» et nøkkelbegrep når det gjelder media og personvern. I forhold som mangler allmenn interesse, ser vi flere eksempler på at det anses retts-

stridig ikke å respektere den omtaltes rett til privatliv. I saker som handler om forhold av allmenn interesse, er det mer sannsynlig at personvernet må vike for ytringsfriheten.

Hva er det så som definerer hva slags forhold i den private sfære som er av «allmenn interesse» og dermed legitimt kan publiseres i mediene? Ifølge Kyrre Eggen (presentasjon for kommisjonen; sml. Eggen 2002 avsnitt 12.4.3.3) er det når forholdet tilfredsstiller minst ett av disse fire kriteriene:

- Når det belyser habilitet.
- Når det belyser eller begrunner maktutøvelse.
- Når det belyser manglende samsvar (diskrepans) mellom utøvelse av makt og egen adferd («diskutabel» ifølge Eggen).
- Når det belyser personlig egnethet til å utøve makt («mer diskutabel» ifølge Eggen).

Videre viser rettspraksis fra EMD (og i økende grad norske domstoler) at verdivurderinger/meningsytringer («value judgments») om offentlige personers personlige egenskaper nyter betydelig beskyttelse under retten til ytringsfrihet, selv om slike meningsytringer er grove og krenker æresfølelsen til den person som omtales (Eggen 2002 del IV).

Skal norsk rettspraksis på dette området endres, må sannsynligvis straffebestemmelsene vedrørende ærekrenkelser endres i skjerpende retning. Justisdepartementet har engasjert Bjørnar Borvik ved Universitetet i Bergen til å skrive en utredning ut fra av et ønske om å endre bestemmelsene om ærekrenkelser hvor intensjonen er nettopp det motsatte; å lempe på reglene, slik at bare grove krenkelser av æresfølelsen og omdømme skal kunne medføre straff (blant annet i tråd med anbefalinger fra Ytringsfrihetskommisjonen). Utredningen til Borvik (*Utredning om det strafferettslige og sivilrettslige vernet mot ærekrenkelser. Forslag til lovbestemmelser i straffeloven 2005 og tvisteloven* – heretter omtalt som «høringsnotat») er sendt ut på høring fra Justisdepartementet (Borvik 2008b). Lovforslaget i høringsnotatet er ment å gi et mer dekkende uttrykk for rettstilstanden slik den er fastlagt i avgjørelser fra EMD. Lovforslaget legger ikke opp til en skjerping av ærekrenkelsesbestemmelsene. En slik skjerping vil kunne komme på kant med EMDs rettspraksis. Personvernkommisjonen mener at en skjerpelse heller ikke er ønskelig fordi det vil gå ut over ytringsfriheten og muligheten til å utsette offentlige personer for kritikk.

Offentlig sfære, privat person

Denne kombinasjonen er særlig problematisk innenfor ulykkes- og kriminaljournalistikken og reiser mange av de samme spørsmål som reportasjer fra den private sfære. Personvernkommisjonen tror at styrking av bevisstheten rundt yrkesetiske retningslinjer kan styrke personvernet på dette området.

13.2 Regulering

Forholdet mellom mediene og personvern er i dag regulert på flere måter. De viktigste nevnes punktvis nedenfor.

1. Gjennom lover, forskrifter og internasjonale konvensjoner.
2. Gjennom rettspraksis.
3. Gjennom forvaltningspraksis.
4. Gjennom selvregulering.
5. Gjennom avtaler.
6. Gjennom allmennmoralen.

I dette kapittelet går vi skjematisk gjennom noen av de mest sentrale bestemmelsene i norsk rett som regulerer personvernet i forhold til mediene. For en generell gjennomgang av den rettslige reguleringen av personvernområdet, se del II.

Lover, forskrifter og internasjonale konvensjoner blir tolket gjennom rettspraksis, nasjonalt og internasjonalt. Vi har i dette kapittelet tatt med noen særlig sentrale avgjørelser i Den europeiske menneskerettighetsdomstol (EMD) og Norges Høyesterett som angår personvern og media.

I Norge suppleres rettspraksisen på personvernområdet med forvaltningspraksis, og da særlig gjennom vedtak i Datatilsynet og Personvernnemnda. Vi vil derfor oppsummere en del sentrale avgjørelser på området.

Norske media driver en utstrakt selvregulering av personvernområdet gjennom Pressens Faglige Utvalg (PFU). Nedenfor drøftes denne selvreguleringen, og den sammenlignes med tilsvarende selvregulering i Storbritannia og Sverige.

I den senere tid har vi sett at ulike aspekter ved individers personvern stadig hyppigere reguleres gjennom eksplisitte avtaler som inngås mellom tjenestetilbyder og brukere av ymse informasjonstjenester. Det er særlig «nye» nettbaserte media som benytter seg av denne formen for regulering.

Til sist ønsker Personvernkommisjonen å gjøre et poeng ut av at i tillegg til de overnevnte, mer eller mindre formelle instrumentene for regulering, så gjenstår det et felt som ikke reguleres av noe annet enn det vi i mangel av et bedre begrep vil kalle «allmennmoralen». Personvernkommisjonen vil peke på at i mange tilfelle kan det være vanskelig å regulere personvernfeltet ved hjelp av formelle instrumenter, og der er det allmennmoralen som gjenstår.

13.2.1 Lover, forskrifter og internasjonale konvensjoner

En sentral lovbestemmelse i norsk rett som regulerer forholdet mellom personvern og media er Grunnloven § 100, om ytringsfriheten. En tilsvarende grunnlovsbestemmelse om personvernet finnes ikke. Begge rettigheter er viktige i en rettsstat og Personvernkommisjonen har derfor anbefalt grunnlovsfesting av personvernet, jf. kapittel 19 og vedlegg 3.

Sentralt er også EMK, som er inkorporert i norsk rett gjennom menneskerettsloven.

Personvernet omtales i EMK art. 8, der første ledd lyder:

> «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.»

Retten til ytringsfrihet er nedfelt i EMK art. 10, som blant annet fastslår:

> «Enhver har rett til ytringsfrihet. Denne rett skal omfatte frihet til å ha meninger og til å motta og meddele opplysninger og ideer uten inngrep av offentlig myndighet og uten hensyn til grenser.»

Ytringsfriheten, slik den er definert i EMK art. 10, er primært en forpliktelse som innebærer at staten skal avholde seg fra å hindre, eller straffe, fri spredning av tanker og ideer. I mange av avgjørelsene fra EMD (jf. nedenfor) har domstolen kommet til at bestemte stater ikke har fulgt opp denne forpliktelsen.

Men en stat har også en forpliktelse til, gjennom et formålstjenlig lovverk, å beskytte ytringsfriheten mot inngrep fra enkeltpersoner eller institusjoner. En begrensning av ytringsfriheten kan være at noen som gir uttrykk for sine meninger i etterkant utestenges fra yrkeslivet, eller møtes med andre sanksjoner.

I den norske Grunnloven, som ble revidert i 2004 som følge av utredningen fra Ytringsfrihetskommisjonen (NOU 1999: 27), er det i tredje ledd gitt et spesielt sterkt vern for «frimodige ytringer». Bestemmelsen gir vern mot inngrep i ytringsfriheten både fra offentlig myndighet *og* fra private (f.eks. arbeidsgivere, foreninger mv.):

> «Frimodige Ytringer om Statsstyrelsen og hvilkensomhelst anden Gjenstand ere Enhver tilladte. Der kan kun sættes slige klarlig definerede Grændser for denne Ret, hvor særlig tungtveiende Hensyn gjøre det forsvarligt holdt op imod Ytringsfrihedens Begrundelser.»

Samtidig fikk Grunnloven § 100 også et sjette ledd – det såkalte infrastrukturkravet:

> «Det paaligger Statens Myndigheder at lægge Forholdene til Rette for en aaben og oplyst offentlig Samtale.»

Om dette heter det i forslaget til ny § 100 (Innst. S. nr. 270 (2003-2004) s. 61):

> «Kravet innebærer at staten aktivt skal medvirke til at individer og grupper har en faktisk ytringsmulighet. Statens oppgave utvides i 6. ledd fra passivt å avstå fra inngrep til aktivt å sikre borgernes ytringsmulighet. Infrastrukturkravet innebærer en forpliktelse til å legge til rette for kanaler og institusjoner og for en åpen og opplyst offentlig samtale, kort sagt et overordnet statlig ansvar for oppbyggingen av et offentlig rom.»

Selv om personvern og ytringsfrihet er tungtveiende hensyn, er de ikke absolutte rettigheter. Dette kommer til uttrykk i både EMK art. 8 annet ledd (gjengitt i kapittel 6.1.3) og EMK art. 10 annet ledd. Sistnevnte, om ytringsfriheten, lyder:

> «Fordi utøvelsen av disse friheter medfører plikter og ansvar, kan den bli undergitt slike formregler, vilkår, innskrenkninger eller straffer som er foreskrevet ved lov og som er nødvendige i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, territoriale integritet eller offentlige trygghet, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, for å verne andres omdømme eller rettigheter, for å forebygge at fortrolige opplysninger blir røpet, eller for å bevare domstolenes autoritet og upartiskhet.»

Disse bestemmelsene innebærer med andre ord at ingen av rettighetene gjelder ubetinget.

Personopplysningsloven regulerer i utgangspunktet all behandling av personopplysninger. For mediefeltet finnes det imidlertid et viktig unntak fra lovens virkeområde i § 7. Bestemmelsen

sier at behandling av personopplysninger som utelukkende skjer for kunstneriske, litterære eller journalistiske, herunder opinionsdannende formål, i hovedsak faller utenfor personopplysningslovens anvendelsesområde. Unntaket er tatt inn av hensyn til ytringsfriheten. Personopplysningsloven kommer derfor i liten grad til anvendelse når det er mediene som behandler personopplysninger. Dette gjelder også de nye mediene, som blogger og nettsamfunn, i den utstrekning disse har kunstneriske, litterære eller journalistiske, herunder opinionsdannende, formål.

Forholdet mellom mediene og personvernet reguleres således i større grad av andre lover, i første rekke straffeloven, der de viktigste bestemmelsene er § 390 (vern av privatlivets fred), § 390a (vern mot plagsom opptreden) og §§ 246-254 (ærekrenkelser).

I åndsverkloven § 45c er det tatt inn en personvernbestemmelse som handler om retten til eget bilde. Hovedregelen er at bilder av en person ikke kan gjengis eller vises offentlig uten at den avbildede har samtykket. Bestemmelsen angir imidlertid en del eksplisitte unntak fra dette vernet, for eksempel for bilder som har aktuell og allmenn interesse, for bilder som gjengir forsamlinger eller folketog i friluft, eller bilder der den enkelte person «er mindre viktig enn hovedinnholdet i bildet».

Unntakene som listes opp i åndsverkloven § 45c og unntaket fra personopplysningslovens virkeområde som nevnt ovenfor, innebærer i praksis at «normal» fotojournalistikk kan publiseres på papir og på nett uten samtykke fra de som er avbildet. Dette fordi formålet med virksomheten utelukkende er journalistisk eller opinionsdannende, og videre fordi bildene viser personer eller situasjoner som av ulike grunner befinner seg i nyhetsbildet, og som derfor kan sies å ha «aktuell og allmenn interesse», eller fordi de viser større forsamlinger eller oversiktsbilder der enkeltindividet ikke er i hovedmotivet.

13.2.1.1 Ansvar og ansvarsavskjæring

Uklare ansvarsforhold eller manglende ansvar i forbindelse med krenkelse av personvernet, kan få betydning for ivaretakelsen av de rettighetene som følger av personvernretten. Derfor ønsker vi å se nærmere på hvordan det forholder seg med strafferettslig og sivilrettslig ansvar i mediene, herunder også hva som fritar for ansvar (ansvarsavskjæring).

Både strafferetten og sivilretten har generelle regler om hvem som kan gjøres ansvarlig for ulovlige ytringer. I tillegg finnes det særlige ansvarsregler innenfor spesifikke områder. I noen tilfeller – som for teknisk medvirkning til produksjon av trykt blad og tidsskrift – er kretsen av mulige ansvarlige redusert. I andre tilfeller – som når det gjelder det særlige redaktøransvaret – er det pålagt større ansvar enn det som ellers ville følge av den generelle ansvarslæren.

I norsk rett finnes det en særlig bestemmelse om redaktøransvar i straffeloven § 431. I straffelovens forstand er redaktøren den som treffer avgjørelser om skriftets innhold, uavhengig hva slags benevnelse vedkommende har, se straffeloven § 436.

Redaktøren er strafferettslig ansvarlig for det bladet trykker dersom innholdet er av en slik karakter at det ville ha pådratt redaktøren ansvar etter en annen lovbestemmelse om han hadde kjent innholdet. Eksempelvis er redaktøren ansvarlig for publisering av et ærekrenkende leserinnlegg selv om han ikke har lest det før offentliggjøring. Dersom han var kjent med innholdet, vil han etter omstendighetene kunne straffes direkte etter bestemmelsene om ærekrenkelser, eventuelt for medvirkning. Redaktøren er ikke ansvarlig dersom han kan bevise at han har iverksatt tilstrekkelige tiltak for å føre kontroll med innholdet i teksten, herunder utarbeidet rutiner og retningslinjer som skal gjøre medarbeidere i stand til å vurdere om publiseringen er i samsvar med norsk rett. Eventuelt ansvar må således forankres i lovgivningen for øvrig. Det samme gjelder for publikasjoner uten redaktør.

Redaktøransvaret gjelder i utgangspunktet for «blad eller tidsskrift», jf. straffeloven § 431. Per i dag er det ikke avklart i hvilken grad det gjelder et redaktøransvar for publikasjoner på Internett, jf. Ot.prp. nr. 19 (2007-2008) (*Om lov om redaksjonell fridom i media*), s. 9.

Noen av de norske bestemmelsene som rammer ulovlige ytringer (som for eksempel ærekrenkelser eller rasistiske ytringer) kan også ramme noen av de som medvirker til spredning av ytringen. Dette innebærer at andre enn den opprinnelige ytrer og redaktøren kan gjøres strafferettslig eller sivilrettslig ansvarlig for å medvirke til spredning av slike ytringer. Et slikt medvirkeransvar kan typisk være aktuelt i de tilfellene hvor det ligger ulovlig informasjon fra tredjepart hos en tjenesteyter eller distributør. Imidlertid er det ikke definert noe medvirkningsansvar for krenkelser av privatlivets fred i straffeloven § 390.

For ivaretakelse av de rettighetene som følger av personvernretten er det viktig at det ikke er

uklart hvem som er rett adressat for en klage på en krenkelse, hvem som har mulighet og myndighet til å gripe inn mot en krenkelse, og hvem som kan stilles til ansvar for rettsstridige krenkelser. Av den grunn mener Personvernkommisjonen at spørsmål om ansvar og ansvarsavskjæring, herunder medvirkningsreglene bør klargjøres bedre enn i dag, særlig med tanke på «nye» media og de ulike aktører som bidrar til produksjon og distribusjon av innhold på disse mediene.

Når det gjelder medvirkeransvaret som kan gjøres gjeldende for distributører og tjenesteytere er det i ehandelsloven tatt inn en egen ansvarsavskjæringsbestemmelse som harmoniserer loven med EU-direktiv 2003/31/EF («ehandelsdirektivet») og som gjelder for «informasjonssamfunnstjenester» («information society services»). Dette uttrykket er definert i ehandelsloven § 1 annet ledd (i samsvar med definisjonen i ehandelsdirektivet). Bing (2008, ss. 207-211) og Bainbridge (2007, s. 408) drøfter også dette begrepet. Bing beskriver definisjonen som «komplisert», mens Bainbridge sier at den er «far from clear». En type tjeneste som det er rimelig klart faller inn under definisjonen av «informasjonssamfunnstjeneste», er når en teknisk operatør (tjenesteyter) mot betaling stiller teknisk infrastruktur (datamaskiner og Internett) til disposisjon for en annen (tjenestemottaker) for lagring og publisering av informasjon på vegne av tjenestemottaker. Mer uklart er det imidlertid om hvorvidt aggregatortjenester, søketjenester, hyperlenketjenester, debatttjenester, etc. omfattes av begrepet.

Ehandelsloven § 18 slår fast at en tjenesteyter bare kan straffes for lagring av ulovlig informasjon eller medvirkning til ulovlig virksomhet ved lagring av informasjon, dersom han har utvist forsett. Det følger av rettspraksis og juridisk teori at forsett foreligger dersom handlingen er tilsiktet, eller dersom gjerningsmannen har regnet følgen som sikker eller overveiende sannsynlig. For erstatningsansvar er det krav om forsett eller grov uaktsomhet. Samme paragraf sier videre:

> «Tjenesteyteren er i alle tilfelle straffri eller fri fra erstatningsansvar dersom han uten ugrunnet opphold treffer nødvendige tiltak for å fjerne eller sperre tilgangen til informasjonen etter at forsettet eller den grove uaktsomheten etter første ledd forelå.»

I forarbeidene til ehandelsloven er det redegjort nærmere for når rettsvillfarelse (med hensyn til om ytringen er ulovlig eller ikke) fritar for ansvar. Departementet uttaler at «nettverten som teknisk formidler står i en slik posisjon at det ikke er grunn til å anvende rettsvillfarelsesnormen for strengt», se Ot.prp. nr. 4 (2003-2004) (*Om lov om endringer i lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester (ehandelsloven)*) s. 27. På samme sted uttaler departementet:

> «Dersom nettverten foretar en aktsom vurdering av den aktuelle informasjonen, bør han kunne påberope seg ansvarsfrihet. Tilsvarende også om nettverten har henvendt seg til kompetente organer, som f.eks. Nettnemnda, dersom nettverten selv mangler den nødvendige juridiske kompetanse på området.»

Disse bestemmelsene i ehandelsloven er spesifikke ansvarsavskjæringsregler som avgrenser ansvaret for tilbydere av informasjonssamfunnstjenester. Men fordi bestemmelsene gjør tjenesteyterens ansvarsfrihet betinget av at tilgang til informasjon fjernes eller sperres, har enkelte tjenesteytere rutinemessig valgt å sperre tilgangen til informasjon fra det øyeblikket de mottar en bekymringsmelding som påstår at informasjonen innebærer en ulovlig ytring, og på den måten overprøver en ansvarlig redaktørs redaksjonelle suverenitet. Et eksempel på dette er teletilbyderen Imbera, som i februar 2008 grep inn i det redaksjonelle innholdet til nettstedet til Human Right Services og fjernet flere artikler fra forsiden som omhandlet karikaturene av profeten Muhammed (Teknofil 2008).

Praksisen på dette området varierer fra tjenestetilbyder til tjenestetilbyder, men det kan virke som enkelte, og da særlig mindre tjenestetilbydere uten erfaring og redaksjonell kompetanse med hensyn til å vurdere lovligheten av kontroversielt innhold, rutinemessig vil iverksette sperring dersom en partsrepresentant påstår at en ytring kan medføre straff eller erstatning, uten å foreta en selvstendig redaksjonell vurdering av hvorvidt en slik påstand medfører riktighet eller ikke.

I 2002 ble ansvarlig redaktør for nettutgaven av svenske Aftonbladet dømt av Stockholm tingsrätt for «hets mot folkgrupp» (rasisme). Årsaken var at det på nettavisens debattsider *Tyck* av lesere i oktober 2000 var lagt ut fire antisemittiske innlegg. Domstolen kom til at redaktøren var straffe-rettslig ansvarlig for innleggene.

Til forskjell fra mange av sine konkurrenter hadde Aftonbladet valgt å forhåndsredigere debattinnlegg på nettsidene. Men de som redigerte innleggene hadde slurvet, og slapp gjennom innlegg som burde vært stoppet. Jungkvist (2002)

forklarer årsaken til at de rasistiske ytringene slapp igjennom forhåndsredigeringen slik:

> «Med det enorma antal inlägg som varje dag skickas till oss blir det med nödvändighet ett grovmaskigt nät. De flesta olämpliga inlägg sorteras bort, men det kan hända att något tar sig igenom kontrollen.»

Tilsvarende grove og rasistiske ytringer har også blitt publisert på debattsidene i andre svenske og norske nettaviser som ikke forhåndsredigerer sidene (Amagasinet 2008). Ofte opptrer de som ytrer seg i slike debatter under fingerte eller falske identiteter. Dette har så langt ikke resultert i noen strafferettslige reaksjoner etter det Personvernkommisjonen kjenner til. Redaktøren som har det formelle ansvaret for det norske nettstedet Hegnar Online, hevder at han ved *ikke* å forhåndsredigere debattsidene er fritatt fra det særlige redaktøransvaret (Bergens Tidene 2008). Dette medfører at både grove ærekrenkelser og andre ytringer som krenker personvernet jevnlig blir publisert på Hegnar Online.

Resonnementet som redaktøren fremfører, er altså at bare dersom en nettbasert publikasjon rent faktisk forhåndsredigeres (ved at et menneske på selvstendig grunnlag eller etter instruks, treffer avgjørelser om hva som publiseres), har en slik publikasjon en redaktør og er følgelig også omfattet av det særlige redaktøransvaret. I fraværet av en slik forhåndsredigering finnes det ikke noe særlig redaktøransvar, og nettpublikasjonen har bare et alminnelig aktsomhetsansvar som innebærer at det rekker å fjerne ulovlige ytringer i etterkant, når staben blir gjort oppmerksom på dem av brukere og lesere. Dette resonnementet har imidlertid ikke vært prøvet for norsk rett. I et forsøk på å få dette spørsmålet rettslig prøvet, har statsviter Bernt Hagtvet anmeldt Hegnar Online og dets redaktør for rasisme (ibid.) på bakgrunn av konkrete ytringer som har blitt publisert på nettstedet. Saken ble henlagt av politiet som intet straffbart forhold. Kommisjonen er ikke kjent med om dette er begrunnet i en vurdering av hva som ligger i redaktørbegrepet eller om det er begrunnet i usikkerheten med hensyn til om nettpublikasjoner omfattes av straffelovens bestemmelser om «blader og tidsskrifter». På strafferettens område vil legalitetsprinsippet stille krav til klarheten i ordlyden og hindre en utvidende tolkning av denne

Ytringsfrihetskommisjonen (1999) tok til ordet for at ansvar og ytringsfrihet bør reguleres av en medieansvarslov for alle media. Personvernkommisjonen vil i denne sammenhengen påpeke at for ivaretakelse av de rettighetene som følger av personvernretten bør det i enhver sammenheng være enkelt for den som er krenket å identifisere og kontakte et ansvarssubjekt som kan gjøres ansvarlig for rettstridige ytringer. Gjennom å regulere ansvarsforholdene i en egen medieansvarslov i stedet for spredt i lovgivingen, tror vi dette kan avklares på en tilfredsstillende måte. Det er dessuten viktig å få likestilt alle typer media, slik at «blader og tidsskrifter» ikke vurderes annerledes enn andre publikasjoner, for eksempel på nett.

13.2.2 Rettspraksis

Nedenfor tar vi for oss rettspraksis fra de to mest sentrale instansene som definerer grensene mellom personvern og ytringsfrihet i norsk rett, nemlig Den europeiske menneskerettighetsdomstol (EMD) og Norges Høyesterett.

Retten til privatliv ifølge EMK art. 8 kan begrenses dersom inngrepet har et rettslig grunnlag og er nødvendig i et demokratisk samfunn for å ivareta noen nærmere angitte formål, inklusive beskyttelse av «andres rett og friheter». Dermed legges det til rette for en ordning som tillater en balansering av ulike rettigheter, slik at man i en konkret situasjon kan avgjøre hvilken rettighet som skal ha forrang.

13.2.2.1 Rettspraksis fra Den europeiske menneskerettighetsdomstol

Den europeiske menneskerettighetsdomstol legger vekt på flere faktorer når den avveier personvern mot ytringsfrihet. Schartum og Bygrave oppsummerer de viktigste avveiningsmomenter slik (Schartum og Bygrave 2006, s. 74, fotnoter utelatt):

> «I avveiningen mellom hensynet til ytringsfrihet og personvernhensyn legger EMD vekt på en lang rekke momenter, deriblant ytringens karakter (er den f.eks. en verdivurdering (<value judgment>) eller en faktisk påstand (<factual statement>)?), ytringens form og medium (er den f.eks. audiovisuelt eller ren tekst?), ytringens kontekst (foreligger det eksempelvis et <climate of continual harrassment>?), emnet for ytringen (gjelder den f.eks. omtale av en offentlig person eller privatperson?) og ytrerens formål (har f.eks. ytreren til hensikt å fokusere på en sak av allmenn interesse eller kun å sjikanere andre?). […] Vektlegging av momentene og deres samspill varierer naturligvis fra sak til

sak. Likevel kommer det frem av EMDs praksis at det sentrale momentet er hvorvidt ytringen bidrar til en debatt av generell samfunnsinteresse. Jo mer en ytring bidrar i så måte desto mer vern vil den få på bekostning av personverninteresser.»

I det følgende beskriver vi en del viktige avgjørelser som illustrerer vektleggingen og operasjonaliseringen av disse momentene i saker som angår media.

Vern av privatlivets fred

EMK artikkel 8 oppstiller en rett til å være i fred. Denne retten omfatter blant annet en beskyttelse mot å bli fotografert eller avlyttet i private sammenhenger. Videre omfatter den beskyttelse mot å få fotografier, videoer eller lydopptak av privat karakter offentliggjort eller brukt i uvedkommende sammenhenger. Retten til å være i fred kan dog måtte vike for sterke motstridende interesser, særlig når det gjelder å forebygge og etterforske kriminalitet, men også i forhold til ytringsfriheten.

I saken *von Hannover mot Tyskland* (dom 2004-06-24) tok EMD stilling til spørsmålet om statenes ansvar for å gi den enkelte lovbeskyttelse mot plagsom oppmerksomhet. Saken gjaldt offentliggjøring av bilder av prinsesse Caroline av Monaco, som såkalte paparazzi-fotografer hadde tatt av henne i ulike private og hverdagslige situasjoner, dvs. utenom offisielle oppdrag. Tyske domstoler hadde kommet fram til at slike bilder kunne offentliggjøres. EMD kom til at bildene var omfattet av ytringsfriheten, men at de var følsomme i forhold til den personlige integriteten. Domstolen mente derfor at en avveining mellom disse interessene måtte gjøres. Domstolen fastslo at grensen mellom ytringsfriheten og beskyttelsen av den personlige integriteten må trekkes basert på i hvilken grad bildene har allmenn interesse. Offentlige personer må tåle mer publisitet enn «vanlige» mennesker, men når den informasjon som formidles ikke bidrar til en debatt av allmenn samfunnsmessig interesse, er offentliggjøringen ikke berettiget. Domstolen mente at spredningen av bildene hadde som eneste formål å tilfredsstille nysgjerrigheten hos leserne med detaljer om prinsessens privatliv og at bildene ikke bidro til en debatt av «general interest». Domstolen mente derfor at det i slike tilfeller er berettiget med en innskrenking av ytringsfriheten og at avisenes kommersielle interesser måtte vike til fordel for beskyttelse av den personlige integriteten. Ifølge EMD innebærer beskyttelsen i EMK artikkel 8 at enhver person, inkludert offentlig kjente personer, skal ha en rett til å utvikles i forhold til andre mennesker, uten uberettiget innblandning fra utenforstående. Tyskland ble funnet skyldig i brudd mot EMK artikkel 8 da landet ikke hadde gjort en korrekt interesseavveining etter EMK, og dermed heller ikke hadde sørget for lovgivning som kunne beskytte den enkeltes private sfære i den grad som EMK krever.

Utlevering av personopplysninger

Utlevering av personopplysninger til media, og da særlig sensitive personopplysninger, som opplysninger om seksuell legning, sykdommer, politisk oppfatning, kriminalitet eller misbruk av rusmidler, kan innebære brudd på EMK art. 8.

Saken *Peck mot UK* (dom 2003-01-28) dreide seg om en kommune i England som hadde utplassert overvåkningskameraer. Peck, som var psykisk ustabil, var ute på natten og viftet med en kniv og ble fanget opp av kameraene. Bildene av ham ble utgitt til enkelte media for å vise hvor effektive kameraene var til å fange opp en farlig kriminell. Peck var imidlertid ute i et meget privat ærend – han hadde tenkt å begå selvmord. EMDs avgjørelse retter seg mot kommunens utlevering av filmmateriale til media og fastslår at dette var en krenkelse av Pecks privatliv.

I saken *Craxi (nr. 2) mot Italia* (dom 2003-07-17) tok EMD stilling til en klage på at Italia ikke hadde etterforsket og straffet personer som hadde forårsaket at konfidensielle opplysninger tilfløt pressen. De konfidensielle opplysningene var utskrifter av private telefonsamtaler som hadde blitt fremlagt som bevis i en rettssak. De ansvarlige hadde ikke gjort noe forsøk på å fjerne avsnitt med sensitive personopplysninger som var irrelevante for saken. EMD kom til at dette brøt med EMK art. 8.

Ærekrenkelser

Mange av de avgjørelsene som EMD har fattet i saker vedrørende media, ytringsfrihet og personvern, dreier seg om ærekrenkelser og vern av omdømme.

Domstolen har i flere saker uttalt at omdømme er del av retten til privatliv som EMK art. 8 oppstiller (se generelt (Borvik 2008a), avsnitt 2.6.3). Omdømme er videre nevnt konkret i EMK art. 10, der det sies at ytringsfriheten kan innskrenkes for å verne andres omdømme.

At omdømme er omfattet av art. 8 fremgår for eksempel av saken *Radio France og andre mot Frankrike* (dom 2004-03-30), der EMD legger følgende til grunn:

> "The Court would observe that the right to protection of one's reputation is of course one of the rights guaranteed by Article 8 of the Convention, as one element of the right to respect for private life."

Saken handlet om nyhetsbulletiner fra en radiostasjon som refererte påstander fra et annet medium om at en prominent fransk politiker hadde bistått tyskerne med deportasjon av franske jøder under krigen. I de korte bulletinene ble det referert til et intervju med den omtalte politikeren, men ikke opplyst om at denne i nevnte intervju benektet beskyldningene. Radiostasjonen ble i fransk rett dømt for ærekrenkelser, og denne dommen ble klaget inn for EMD. Sistnevnte kom til at dette ikke brøt med EMK art. 10.

Det er lite tvilsomt at EMK art. 8 innebærer at stater som har sluttet seg til EMK er forpliktet til å vedta lover som beskytter den enkelte mot ryktespredning, injurier eller andre former for nedsettende omtale. Det er derimot fortsatt uavklart hvordan slike lover skal tolkes i saker der slik omtale har, eller kan ha, allmenn interesse, eller hva som er å anse som en straffbar ærekrenking og hva som er en ren meningsytring. Det er videre uavklart hvorvidt *æresfølelsen* har et selvstendig konvensjonsrettslig vern etter EMK artikkel 8 (jf. (Borvik 2008b), avsnitt 2.1.3; sml. (Borvik 2008a), avsnitt 2.6.2).

De siste års rettspraksis fra EMD, og ikke minst det faktum at Norge har fått flere fellende dommer mot seg i klagesaker vedrørende EMK art. 10, har bidratt til at norske myndigheter ønsker å endre på de norske reglene om ærekrenkelser. Borvik (2008b) skriver:

> «Disse dommene fra EMD virker selvsagt også inn på handlingsrommet til den norske lovgiveren og de norske domstolene. Ytringsfrihetskommisjonen tok i NOU 1999:27 på s. 114 til orde for å bygge ned det rettslige vernet mot ærekrenkelser, noe departementet på generelt grunnlag sluttet seg til i St.meld. nr. 26 (2003–2004) på s. 49.»

I sin rettspraksis i saker som handler om ærekrenkelser har EMD fokusert på graden av allmenn interesse. Når en sterk allmenn interesse gjør seg gjeldende må det krav som enkeltpersoner har for beskyttelse av sitt rykte og sitt privatliv vike. En slik allmenn interesse er hensynet til den frie politiske debatten, som må gi rom for kritikk av personer i fremtredende roller i politikken, samfunnslivet og forretningslivet, også i spørsmål som angår deres adferd og moral i andre og tidligere sammenhenger.

Når det gjelder spørsmål om offentliggjøring av opplysninger om personlige forhold, anser EMD det slik at folk som innehar offentlig embete, eller som selv velger offentlighetens rampelys, må regne med å bli gjenstand for mer nærgående oppmerksomhet enn folk i alminnelighet. EMD har blant annet behandlet spørsmål om offentliggjøring av fotografier, lønnsopplysninger og konfidensielle helseopplysninger som handlet om kjente personer, og kommet til at publiseringen må tillates av hensyn til allmenn interesse.

På bakgrunn av dette har EMD i flere tilfeller overprøvd avgjørelser av nasjonale domstoler som har dømt media for ærekrenkelser. Ett eksempel er *Lingens mot Østerrike* (dom 1986-07-08). Lingens ble bøtelagt etter østerriksk lov for å ha satt på trykk flere svært negative karakteristikker av den Østerrikske kansleren, som «umoralsk» og lignende. Bakgrunnen for boten var at Lingens ikke kunne føre sannhetsbevis for sine påstander, noe som var påkrevd etter østerriksk lov. EMD kom til at det var nødvendig å skille mellom fakta og verdivurderinger/meninger. Lingens ytringer var verdivurderinger. Vurderinger er subjektive og kan ikke bevises, og dermed var det galt av rettsapparatet i Østerrike å kreve sannhetsbevis for påstandene. EMD fastslo videre at politikere har rett til beskyttelse mot ærekrenkelser, men at de sammenlignet med mange andre er nødt til å tåle langt skarpere vurderinger av sin person og moral.

EMD har også behandlet flere saker som faller utenfor den politiske arena, der journalister eller enkeltpersoner gjennom avisartikler eller på annen måte har gått ut med påstander om uregelmessigheter i offentlig virksomhet eller varslet om klanderverdige forhold, og på grunnlag av dette blitt dømt for ærekrenkelser. Gjennomgående for disse sakene er at EMD har kommet til at dommene strider med EMK art. 10 og ytringsfriheten dersom påstandene har omhandlet forhold av allmenn interesse og vært tilstrekkelig dokumentert.

For eksempel i saken *Bergens Tidende mot Norge* (dom 2000-05-02) hadde Bergens Tidende skrevet en serie artikler om en plastisk kirurg som ifølge avisen feilbehandlet sine pasienter. Norges høyesterett kom til at avisen var skyldig i

ærekrenkelser, og tilkjente legen erstatning. Høyesterett uttalte at direkte feilaktige faktiske opplysninger av negativ karakter vil måtte betraktes som ærekrenkelser, og anså det ikke som unnskyldende at avisen bare gjentok en annens beskyldninger. EMD kom imidlertid til at i denne saken gikk allmennhetens interesser av å få vite om mulig feilbehandling foran legens interesse i å beskytte sitt omdømme, og at journalisten var i god tro da han videreformidlet de feilaktige faktiske opplysningene. Domstolen la vekt på at det dreide seg om helsespørsmål av betydning for offentligheten og at forholdet således ikke var en sak mellom de involverte personer og legen alene. Et større fokus på enkeltpersoner kan således aksepteres dersom saken gjelder forhold av allmenn interesse. Det fremheves av domstolen at EMK artikkel 10 også verner ytringer som kan virke fornærmende, sjokkerende eller urovekkende.

I saken *White mot Sverige* (dom 2006-09-19) hadde White i artikler i to svenske aviser feilaktig blitt anklaget for å være delaktig i mordet på Olof Palme. White saksøkte, men svensk rett ga ham ikke medhold. White fikk da EMD til å vurdere om svensk lovgiving ga god nok beskyttelse mot spredning av ærekrenkende rykter. EMD fant imidlertid at det samlede bildet som avisene hadde formidlet var balansert og at den allmenne interesse i denne saken måtte veie tyngre enn hensynet til Whites omdømme.

I saken *Radio Twist, A.S. mot Slovakia* (dom 2006-12-19) kom EMD til at publisering av en telefonsamtale mellom en statssekretær og en minister som var tatt opp på ulovlig vis var vernet av ytringsfriheten, fordi samtalen dreide seg om forhold av allmenn interesse.

I saken *Tønsberg Blad AS og Haukom mot Norge* (dom 2007-03-01) hadde avisen publisert en reportasje om manglende etterlevelse av boplikt i Tjøme kommune, og i samband med dette publisert navnene på en liste over utvalgte personer som skulle kontrolleres i forbindelse med boplikt. Listen var utarbeidet av kommunen. En tidligere direktør i et stort norsk konsern befant seg på denne listen og gikk til sak med krav om mortifikasjon av og oppreisning for ærekrenkende utsagn. Høyesterett mente at avisen hadde fremsatt en usann ærekrenkende beskyldning om faktiske forhold og at ytringene ikke var vernet av EMK art. 10. Det ble lagt vekt på at beskyldningen hadde begrenset allmenn interesse. Selv om vedkommende på listen var en forholdsvis kjent person presiserte Høyesterett at dette ikke innebærer at han uten videre kunne anses som en offentlig person i forhold til bopliktreglene. EMD hadde en annen oppfatning når det gjaldt spørsmålet om ytringen var av offentlig interesse. Domstolen presiserte at mulig brudd fra fremtredende personer på regler som har til hensikt å beskytte viktige offentlige interesser, i visse tilfeller kan ha allmenn interesse.

Det finnes imidlertid også avgjørelser som peker i annen retning. Vi har allerede nevnt *Radio France og andre mot Frankrike*.

I saken *Campmany y Diez de Revenga og Lopez-Galiacho Perona mot Spania* (dom 2000-12-12) ble to journalister av spansk domstol dømt til å betale erstatning for at de hadde publisert opplysninger om en intim forbindelse mellom to kjente personer og fotografier som støttet opp om disse opplysningene. EMD kom til at dommen mot journalistene ikke krenket ytringsfriheten ettersom opplysningene dreide seg om private forhold som manglet allmenn interesse.

Vi kan oppsummere med at EMDs avgjørelser på dette området legger til grunn at dersom det foreligger tilstrekkelig sterke allmenne interesser for at opplysninger som svekker en persons omdømme offentliggjøres, så må beskyttelsen av privatlivet (og omdømme) i EMK art. 8 vike for ytringsfriheten i EMK art. 10. Når det ikke foreligger slike interesser, eller når pressen videreformidler usanne ærekrenkende påstander, uten å være i god tro med hensyn til påstandens riktighet, er ytringsfriheten innskrenket til fordel for privatliv og/eller omdømme.

13.2.2.2 Rettspraksis fra Norges Høyesterett

Retten til eget bilde

I Rt 2001 s. 1691 (*teazer.tv-kjennelsen*) behandlet Høyesteretts kjæremålsutvalg i desember 2001 en sak som gjaldt åndsverkloven § 45c og rett til visning av fotografi når de avfotograferte ikke hadde gitt sitt samtykke til dette. Gjengivelsen hadde skjedd på et nettsted (teazer.tv), som markedsfører seg selv som et pornografisk nettsted. På nettstedet var det lagt ut et bilde av to tidligere deltagere i et tv-program, tatt under et moteshow i Oslo. Kjæremålsutvalget kom enstemmig til at åndsverkloven § 45c forhindret at bildet kunne benyttes uten de avbildede personenes samtykke. Kjæremålsutvalget begrunnet dette i at hensynet til ytringsfriheten (jf. Grunnloven § 100 og EMK art. 10) ikke tilsa noen innskrenkende tolkning av åndsverkloven § 45c bokstav a («avbildningen har aktuell og allmenn interesse») i forhold til den aktuelle bruk. I dommen heter det:

> «Det nærmere innhold i bestemmelsen må fastlegges ved en interesseavveining der i første rekke allmennhetens informasjonsbehov veies mot den avbildedes interesse i vern mot bruk i sammenhenger som er urimelig belastende.»

Kjæremålsutvalget veier her ytringsfriheten opp mot hvor viktig ytringer er fra et samfunnsmessig synspunkt. Hvorvidt «avbildningen har aktuell og allmenn interesse» avhenger altså av to ting: «allmennhetens informasjonsbehov» (informasjon om viktige samfunnsspørsmål må komme fram i mediene) og det vernet den som er avbildet skal ha mot å få sitt bilde benyttet i en krenkende sammenheng. Det forholdet at ytringen i dette tilfelle var uviktig, og at bildet ble benyttet i en pornografisk kontekst, ble utslagsgivende for den fellende dommen.

Retten til eget bilde er også drøftet i saken HR-2008-01480, som refereres nedenfor.

Vern av privatlivets fred

I Rt 2007 s. 687 (*Big-brother-kjennelsen*) behandlet Høyesterett en sak om hvorvidt *Se og Hør* gjennom tre reportasjer sommeren 2003 rettsstridig hadde krenket privatlivets fred overfor to tidligere deltagere i fjernsynsserien *Big-brother*.

I Høyesteretts vurdering av saken sto EMDs avgjørelse i *von Hannover mot Tyskland* sentralt.

Høyesterett la til grunn at rettsstridskravet etter straffeloven § 390 må forstås slik at det samsvarer med kravene i EMK art. 8 om retten til privatliv og art. 10 om ytringsfrihet. Etter å ha tolket dommen fra EMD, konstaterte Høyesterett at det helt sentrale når det gjelder vern av privatlivet, er om oppslaget gir et bidrag til en debatt av allmenn interesse. Videre ble det lagt til grunn at personvernet står sterkt i forhold til ytringsfriheten ved omtale av personer som ikke har samfunnsfunksjoner. EMK art. 10 skal verne om samfunnsdebatten og demokratiet, ikke adgangen til å legge fram opplysninger om personlige forhold om privatpersoner, selv om de er kjente. Høyesterett la til grunn at Big-brother-paret var kjente personer, men at de ikke sto for samfunnsfunksjoner. Fordi de gjennom fjernsynsserien *Big-brother* hadde valgt rampelyset, måtte de finne seg i nærgående omtale under sendingene og en tid etter dette, men Høyesterett mente det samme ikke kunne gjelde to år etter at sendingene var slutt og ett år etter at de hadde sluttet å la seg intervjue. Retten mente videre at selv om terskelen for hva som vil være tilstrekkelig sensitivt til å rammes av § 390 vil være noe hevet for personer som hadde deltatt i et program som *Big-brother*, ledet tidspunktet og innholdet i Se og Hørs første artikkel til at det innebar en klar krenkelse av privatlivets fred å skrive om et mulig samlivsbrudd mellom de to.

I dommen er det lagt til grunn at kjerneområdet for vernet etter straffeloven § 390 gjelder formidling av sanne opplysninger om personlige forhold, men at bestemmelsen også verner mot formidling av usanne opplysninger. Om betydningen av sannhet er det uttalt at:

> «Det sentrale for vernet er om det ligg føre ei krenking av privatlivs fred, og ikkje om opplysningane er sanne eller ikkje.»

Høyesterett fant at ingen av reportasjene ga noe tilskudd til den offentlige debatten og at samtlige artikler innebar en rettsstridig krenkelse av privatlivets fred. Det ble ikke lagt noen vekt på at PFU hadde konkludert med at reportasjene lå innenfor det som er tillatt etter Vær Varsom-plakaten.

Før saken ble behandlet av Høyesterett hadde reportasjene blitt behandlet i PFU (PFU-sak 083/03). PFU fant at et oppslag om at forholdet var slutt ikke brøt med god presseskikk. PFU fremholdt i sin uttalelse:

> «På den annen side finner utvalget å måtte legge vekt på at klagerne aktivt og i uvanlig sterk grad har søkt offentlighet, og selv skapt omfattende publikumsinteresse for hvordan forholdet mellom dem ville utvikle seg. Sett på denne bakgrunn anser utvalget at klagerne må tåle større og endog mer belastende oppmerksomhet omkring sitt privatliv enn mennesker som ikke har satt seg i en slik situasjon. Etter utvalgets mening har klagerne, sammen og hver for seg, selv bidratt til å skape uklarhet om forholdet.»

I HR-2008-647-A (april 2008) vurderte Høyesterett igjen forholdet mellom EMK artikkel 8 og artikkel 10 i den såkalte «*Plata-kjennelsen*». Saken dreide seg om et innslag på NRK TV der en person på Plata i Oslo ble filmet mens politiet pågrep ham for kjøp av heroin.

De aktuelle opptakene i saken stammet fra politiets overvåkning av Plata, og deler av dette materialet ble gjort tilgjengelig for NRK i forbindelse med en konkret politiaksjon.

Høyesterett la her avgjørende vekt på at det forelå sterk allmenn interesse i det aktuelle innslaget på NRK. Konteksten for innslaget ble tillagt

stor vekt, ved at NRK hadde fokusert på den alminneliggjøringen av omsetning av narkotika som videosekvensen gir uttrykk for. Dette var et viktig innspill i en pågående debatt i samfunnet omkring nettopp dette spørsmålet.

Høyesterett viser helt konkret til at *Big-brother-kjennelsen* gjaldt en reportasje som bar preg av sladder, med tilhørende svak grad av allmenn interesse. *Plata-kjennelsen* gjaldt derimot spørsmål av samfunnsmessig betydning. Dermed forelå det et vern under ytringsfriheten.

I HR-2008-01480-A (september 2008) vurderte Høyesterett for tredje gang på kort tid forholdet mellom EMK artikkel 8 og artikkel 10 i en sak om betaling av oppreising for brudd på straffeloven § 390 og åndsverksloven § 45c i den såkalte *bryllupsfoto-kjennelsen* («Se og Hør Forlaget AS mot Lars Lillo-Stenberg og Andrine Sæther»).

Saken var foranlediget av Se og Hørs reportasje om bryllupet mellom skuespiller Andrine Sæther og musiker Lars Lillo-Stenberg. Artikkelen inneholdt både tekst og bilder fra tiden før og etter vielsen. Paret hadde ikke samtykket til reportasjen. Paret hadde fått medhold i både Tingretten og Lagmannsretten, men Høyesterett kom med et knapt flertall til motsatt resultat.

Flertallet på tre dommere konkluderte med at det ikke forelå en krenkelse av privatlivets fred, selv om det dreide seg om opplysninger som samlet sett vedrørte forhold av personlig karakter og som gjaldt privatlivet. Flertallet kom videre til at det ikke forelå krenkelse av retten til eget bilde.

I sin vurdering av om reportasjen var rettstridig sammenholdt førstvoterende saken opp mot tidligere rettspraksis fra Norge og EMD, særlig *Big-brother-kjennelsen* og *von Hannover mot Tyskland*. Det ble lagt vekt på at innholdet i reportasjen var av nøytral karakter, uten noen form for kritikk, og ikke inneholdt noe som kunne fremstå som belastende for ektefellene eller svekke deres omdømme. Dette i motsetning til i *Big-brother-kjennelsen* hvor det forelå flere reportasjer av mer invaderende karakter om det private samlivet. Det ble også fremhevet at bryllupet fant sted på et allment tilgjengelig område, i tillegg til at det ble benyttet virkemidler (kor, båt etc.) som påkalte oppmerksomhet og ga det hele et spektakulært preg. Ektefellene kunne således ikke ha en forventning om at de var skjermet på noen måte.

Mindretallet i Høyesterett (to dommere) konkluderte med at reportasjen krenket det vern av privatlivet som følger av straffeloven § 390. Disse mente at selv om bryllupet skjedde på et sted hvor offentligheten i utgangspunktet har tilgang, følger det av praksis fra EMD at vernet om privatlivet også kan gjelde på steder som er offentlig tilgjengelige. Det ble fremhevet at de ytre rammene gjorde at dette bar preg av å være en privat vielsesseremoni som må betraktes som et «personlig forhold» i henhold til straffeloven § 390. I rettsstridsvurderingen ble det lagt vekt på at reportasjen ikke syntes å gi noen bidrag til samfunnsdebatten selv om den omhandlet kjente personer innenfor norsk kulturliv.

Eksemplene på rettspraksis viser at det ofte kan være vanskelig å forutsi hva utfallet av saker som gjelder forholdet mellom personvern og ytringsfrihet vil bli. Dette skyldes at det må foretas en skjønnsmessig avveining av flere momenter.

13.2.3 Forvaltningspraksis

Forholdet mellom personvern og ytringsfrihet er også gjenstand for vurdering i forvaltningen, da særlig i saker som behandles av Datatilsynet og Personvernnemnda. Kompetansen til disse organene er imidlertid avgrenset av det mandat de er gitt gjennom personopplysningsloven. Som nevnt ovenfor, er personvern langt mer enn personopplysningsvern. Videre avgrenses kompetansen ytterligere av personopplysningsloven § 7. Her er det bestemt at behandling av personopplysninger som utelukkende skjer for kunstneriske, litterære eller journalistiske, herunder opinionsdannende formål, i hovedsak faller utenfor personopplysningslovens anvendelsesområde. Dette innebærer blant annet at en rekke ytringer som krenker personvernet ikke kan behandles av Datatilsynet og Personvernnemnda, fordi de faller utenfor deres kompetanseområde. Eksempler på slike ytringer er foreldres kritikk av barnevernet i en form som krenker eget barns eller ansatte i barnevernets personvern og ulike former for grov mobbing og sjikane som i tillegg har karakter av å ha kunstneriske eller opinionsdannende formål. Vi utdyper disse og andre eksempler nedenfor. Selv om slike ytringer ikke rammes av hovedbestemmelsene i personopplysningsloven, er de ikke nødvendigvis lovlige, og kan for eksempel rammes av bestemmelser i straffeloven eller i åndsverkloven.

Nedenfor nevner vi de viktigste sakene som har vært til behandling i Personvernnemnda, og som omhandler forholdet mellom personvern og ytringsfrihet og tolkningen av personopplysningsloven § 7.

PVN-2005-03: Saken gjaldt et nettsted som inneholdt kritiske kommentarer til behandlingen

av barnevernsaker og relaterte spørsmål. På siden var det blant annet lister over psykologer, barnevernansatte, advokater etc. som hadde hatt befatning med konkrete barnevernsaker. Disse ble fremstilt i et svært kritisk lys. To personer som ønsket sitt navn fjernet fra listen, klaget saken inn for Datatilsynet. Tilsynet avviste saken med den begrunnelse at ytringene lå i grenseland mellom ytringsfrihet og personvern og henviste til at det var tvilsomt hvorvidt Datatilsynet hadde kompetanse til å gjøre inngrep i ytringsfriheten i slike tilfeller.

Personvernnemnda kom til at behandling av personopplysninger på nettstedet falt inn under unntaket i personopplysningsloven § 7. Nemnda fant det klart at nettstedet representerte en virksomhet med opinionsdannende formål selv om man forsøkte å påvirke opinionen på en annen måte enn det man ville forvente for eksempel i en dagsavis. Personvernnemnda presiserte at nettstedene, i likhet med andre media, må overholde og respektere bestemmelser som gjelder omtale av enkeltpersoner, blant annet bestemmelser om privatlivets fred og ærekrenkelser i straffeloven. Krav om sletting av personopplysninger på nettstedet ble således ikke tatt til følge.

PVN-2007-05: Det ovenfor nevnte nettstedet med kritisk blikk på barneverntjenesten ble også gjenstand for behandling i Personvernnemnda i 2007. Denne gangen gjaldt klagesaken publisering av opplysninger om fosterforeldre. Datatilsynet fattet vedtak om at publisering av personopplysninger på dette nettstedet falt inn under unntaket i personopplysningsloven § 7. Selv om nettstedet var vurdert å ha et opinionsdannende formål i tidligere klagesak, foretok tilsynet en konkret vurdering hvor man så hen til fosterforeldres rolle i barneverntvister og deres forhold til barneverntjenesten som profesjonelle aktører. Det ble konkludert med at informasjon om disse ble publisert for å oppnå det samme som ved publisering av opplysninger om barnevernansatte, advokater etc.

Nemnda var enig i Datatilsynets vurderinger. Det var på det rene at fosterforeldrenes oppførsel, utseende etc. var kommentert på nettsiden og at dette kunne føles belastende, men dette måtte likevel sies å ligge innenfor ytringsfrihetens rammer. Personvernnemnda presiserte at det ikke er ønskelig å gjøre denne formen for ytringer til gjenstand for forhåndsvurderinger, dvs. sensur.

PVN-2005-14: Saken gjaldt en klage fra en privatperson på publiserte personopplysninger på et nettsted. Siden inneholdt navn og gradering innenfor en bestemt karatestilart og var administrert av en stilartsorganisasjon. Datatilsynet ga pålegg om sletting under henvisning til at nettstedet ikke kunne karakteriseres som journalistisk virksomhet. Personvernnemnda kom til at klubbens hjemmeside var omfattet av personopplysningsloven § 7 og denne bestemmelsens begrep «journalistisk formål»; og dermed unntatt slettereglene i personopplysningsloven. Klager kunne derfor ikke kreve at personopplysningene skulle slettes. Nemnda uttaler at et motsatt resultat ville medført at en person kan «redigere» historien og gjøre den ufullstendig.

PVN-2006-2: En person ønsket sine leserinnlegg på et nettbasert debattforum tilhørende en regionavis slettet. Innleggene hadde resultert i flere motinnlegg fra andre debattanter som klager opplevde som sjikanerende. I tillegg krevde vedkommende sletting av alle registreringer som var relatert til klagers navn gjennom søkemotoren Google. Klager opplevde det som krenkende at søk på vedkommendes navn også resulterte i at motinnleggende ble gjenfunnet. Datatilsynet mente at de ytringer som klager ønsket forfulgt ikke var av en slik art at personopplysningsloven kom til anvendelse. Ytringene ble ansett vernet av ytringsfriheten.

Personvernnemnda kom, i likhet med Datatilsynet, til at ytringer på slike debattsider faller inn under personopplysningsloven § 7. Nemnda så det som klart at slike debattinnlegg har til formål å påvirke opinionen og diskusjonen i den alminnelige samfunnsdebatt. Det ble også lagt vekt på at ytringene var frivillig publisert på debattsiden.

Når det gjaldt det forhold at klagers debattinnlegg også var gjenfinnbart via Google, påpekte nemnda at Google indekserer og katalogiserer alle opplysninger som ligger tilgjengelig på Internett. En regionavis kan neppe påvirke eller hindre slik indeksering.

Til dette siste vil Personvernkommisjonen bemerke at Google (og andre søkemotorer) har mekanismer som legger til rette for at utgiver kan kontrollere hvordan utgivers informasjon indekseres og gjøres tilgjengelig for søk (eventuelt gjøres utilgjengelig for søk). Dette endrer dog ikke på at leserinnlegg på et debattforum utvilsomt faller inn under personopplysningsloven § 7.

13.2.4 Yrkesetiske retningslinjer

Yrkesetiske retningslinjer eller retningslinjer for bestemte profesjoner eller virksomheter tar utgangspunkt i allmennmoralen/folkeskikken (jf.

avsnitt 13.2.6), men er i tillegg en mer systematisk gjennomtenkning av normer og verdier som gjelder for den aktuelle gruppen eller virksomheten. Hensikten med disse er å bevisstgjøre om etiske utfordringer i feltet, gi retningslinjer for ønsket adferd og skape tillit til utøverne og virksomheten som helhet.

Når det gjelder mediefeltet, er det pressens selvregulering gjennom Pressens Faglige Utvalg (PFU) som utgjør de yrkesetiske retningslinjene.

13.2.4.1 PFU

PFU er opprettet av Norsk Presseforbund og har syv medlemmer. Flertallet på fire kommer fra pressen, tre representerer allmennheten. PFU har som formål å overvåke og fremme den etiske og faglige standard i alle typer media.

PFU er ingen domstol, og det er ikke nødvendigvis samsvar mellom PFU og domstolene i skillet mellom rett og galt. Da von Hannover-dommen (jf. avsnitt 13.2.2) ble debattert på redaktørforeningens høstmøte 2006, kom generalsekretær i Norsk Presseforbund, Per Edgar Kokkvold, med et sterkt og kritisk utfall mot dommen. Dommen «er dårlig moralfilosofi, i verste fall politisk synsing», konkluderte han (Grimstad 2008, s. 288). I samband med *Big-brother-kjennelsen* uttalte Kokkvold ifølge VGnett: «I et fritt og demokratisk samfunn må det være pressens egne organer, ikke rettsapparatet som tar stilling til hva som skal publiseres» (VGnett 2004).

I sin presentasjon for kommisjonen fremholdt presseforskeren Svein Brurås at det på den annen side er liten tvil om at det for mange pressefolk oppleves som pinlig og sviende å bli felt av «sine egne» i PFU. En domfellelse, som oftest i en injuriesak, vil ofte føles mindre belastende – og i noen tilfeller endog avstedkomme sympati fra kolleger, der man får et oppmuntrende klapp på skulderen og kan dele en felles mening om at injurielovgivningen truer kritisk journalistikk.

PFUs avgjørelser er i første rekke normdannende. PFU tar sine avgjørelser med utgangspunkt i et eget regelverk som består av Vær Varsom-plakaten, Redaktør-plakaten og Tekstreklame-plakaten.

En person eller organisasjon som er berørt av et medieoppslag og som mener at regelverket er brutt, kan klage mediet som står bak oppslaget inn for PFU. Klagebehandlingen er gratis.

Norsk Presseforbund oppfordrer alltid partene til å snakke sammen før saken oversendes PFU. I en fornuftig dialog blir ofte misforståelser avklart, saken løst og noen tilfeller ender saken med at en beklagelse blir offentliggjort uten PFU-behandling. Hvert år utarbeider PFU statistikk over hvilke media som har vært flest ganger i PFU og hvor mange fellende uttalelser de har fått mot seg. Det regnes som en belastning for et medium å komme høyt opp på denne statistikken. Følgelig er redaktører villig til å strekke seg langt for å oppnå en minnelig ordning dersom det er sannsynlig at en klage vil føre til en fellende uttalelse.

Det vil gå for langt å drøfte organiseringen av tilsvarende selvreguleringsorganer i andre land i detalj, men vi vil kort trekke fram enkelte nøkkeltall i årsmeldingene for 2007 fra britiske *Press Complaints Commission* (PCC) og svenske *Allmänhetens Pressombudsman* (PO) sammen med *Pressens Opinionsnämnd* (PON) og sammenligne dem med tilsvarende tall fra PFU. Siden variasjonene fra år til annet er forholdsvis moderate, mener vi at tallene fra 2007 er representative for de respektive utvalgenes praksis.

I 2007 mottok PCC 4340 klager. Av disse kom 32 til full behandling i utvalget, der 16 førte til fellinger og 16 til frifinnelser. I bortimot halvparten av klagene endte det med en minnelig ordning uten behandling i utvalget. Resten ble enten avvist, lå utenfor mandatet, eller ble behandlet administrativt, fordi sekretariatet mente at de ikke stred mot god presseskikk.

I 2007 mottok PO i fjor 313 klager. Samme år ble 273 klager «avskrevet» av PO, og 44 videresendt for behandling i PON.[1] Samme år behandlet PON 113 saker, der 38 var videresendt fra PO og 75 var ankesaker). Av disse kom 95 til full behandling, og 40 av disse endte med fellende uttalelse, 55 med frifinnende, mens resten ble avvist.

I 2007 mottok PFU 314 klager. Av disse kom 165 til full behandling. 84 av disse endte med frifinnende uttalelser, 75 med fellende uttalelser, og 6 med kritikk, som er en mildere form for felling. I 40 saker ble det inngått minnelig ordning, eller klagene ble trukket av andre grunner.

Som det fremgår, ligger det til grunn svært ulik saksbehandling i de ulike landene. I Storbritannia er klageantallet stort, og det inngås også et svært stort antall minnelige ordninger. I Sverige fungerer PO som førsteinstans, slik at et stort flertall av sakene avvises administrativt. I Storbritan-

[1] Når det gjelder PO og PON i Sverige, så kan klager bli liggende over et årsskifte før de videresendes/behandles, og PON slår også sammen saker. Derfor stemmer ikke antallet klager PON har mottatt med summen av «avskrevet» og «videresendt».

nia kommer bare ca. 0,8 % av klagene til full behandling med uttalelse i PCC. I Sverige blir ca. 30 % behandlet av PON. I Norge er dette tallet 53 % for PFU. Når det gjelder andelen av klager som fører til fellende uttalelse er denne ca. 0,4 % i Storbritannia (PCC), 13 % i Sverige (PON), og 24 % i Norge (PFU).

Vi ser altså at andelen av klager som gis full behandling, og andelen av klagene som fører til fellende uttalelser, er vesentlig høyere i Norge enn i de to andre landene. Personvernkommisjonen har imidlertid ikke sett nærmere på disse sakene og har ikke grunnlag for å uttale seg om i hvilken grad de ulike landenes praksis er egnet til sammenlikning.

Det er ikke nødvendigvis sammenfall mellom PFUs presseetiske retningslinjer og norsk lov. I noen tilfeller er de etiske retningslinjene strengere enn jussen. Det finnes således mange eksempler på at et medium er felt i PFU, men frifunnet i retten (og naturligvis flere eksempler på at et medium er felt både i PFU og i retten). Men det finnes bare ett eksempel på at et medium er gitt medhold i PFU, men dømt i retten. Dette er den såkalte *Big-brother-kjennelsen*, som vi allerede har drøftet i avsnittet om norsk rettspraksis.

Her må det imidlertid bemerkes at de fleste saker føres enten for domstolene eller for PFU, ikke begge steder. Gitt at det ikke nødvendigvis er sammenfall mellom pressens yrkesetiske retningslinjer og norsk lov på personvernområdet, mener Personvernkommisjonen at det er et rettsikkerhetsproblem at bare et fåtall av disse sakene blir prøvet for domstolene. Årsaken er sannsynligvis økonomisk, i og med at PFU-behandling er gratis, mens det kan være store kostnader forbundet med å få prøvet en sak for domstolene.

Det er heller ikke nødvendigvis sammenfall mellom kjennelser i domstolene og allmennmoralen (jf. avsnitt 13.2.6). Høyesterett kom til at Se og Hør holdt seg innenfor norsk lov i den såkalte bryllupsfoto-kjennelsen. Men i avisenes leserbrevspalter og i andre kommentarer fra «vanlige» mennesker er det mange negative reaksjoner på pressens fremgangsmåte (snikfotografering med telelinse) og på at bildene ble publisert uten samtykke fra de som ble avbildet.

Vær Varsom-plakaten

Norsk Presseforbund vedtok den første Vær Varsom-plakaten i 1936. Deretter gikk det 20 år før den ble revidert. Fra 1956 og fram til i dag har Vær Varsom-plakaten blitt revidert flere ganger, siste gang i november 2007. Denne jevnlige revisjonen er et uttrykk for at de presseetiske normer ikke er statiske. Endringene i samfunnet og pressen selv, journalisters oppfatning av egen yrkesrolle og publikums orientering mot nye verdier, gjør at den med jevne mellomrom må revideres. Medlemmer av både Norsk Journalistlag og Norsk Redaktørforening er forpliktet til å etterleve de etiske retningslinjene i Vær Varsom-plakaten.

Redaktør-plakaten

Redaktør-plakaten er en frivillig avtale mellom Mediebedriftenes Landsforening og Norsk Redaktørforening.

I Redaktør-plakaten står det at en redaktør alltid skal ha frie mediers ideelle mål for øye. Redaktøren skal ivareta ytringsfriheten og etter beste evne arbeide for det som etter hans/hennes mening tjener samfunnet. Dette er ikke nødvendigvis sammenfallende med hva som tjener personvernet.

Etter forslag fra kulturminister Trond Giske og regjeringen, vedtok Stortinget våren 2008 «Lov om redaksjonell fridom i media» (den trer i kraft 1. januar 2009), som lovfester det sentrale innholdet i Redaktør-plakaten. Dermed ble prinsippet om redaksjonell frihet lovfestet. I motsetning til bestemmelsene om redaktøransvar i straffeloven, er denne loven forsøkt gitt en teknologinøytral utforming og plikten til å ha redaktør omfatter periodika og kringkastere, samt «elektroniske massemedium som har tilsvarende føremål og funksjon» som periodika og kringkastere (§ 2).

Etter Personvernkommisjonens oppfatning er loven et første skritt på veien mot en bredere *medieansvarslov*, som er bedre oppdatert og tar hensyn til den teknologiske utviklingen, særlig i forhold til elektroniske massemedia. Da familie- og kulturkomiteen behandlet loven i mars 2008, ble det spesielt pekt på behovet for en avklaring på spørsmålet om redaktørens ansvar i forhold til uredigerte nettdebatter. Komiteen ba departementet komme tilbake med en vurdering av dette så snart som mulig.

13.2.4.2 En bredere mediedebatt

Den offentlige mediedebatten i Norge er oppstykket og overfladisk. Den foregår gjerne i og omkring de enkelte publikasjonene, samt i bransjeinterne forum som PFU og redaktørforeningen.

Terje Angelshaug, som er leserombud i Bergens Tidende, har foreslått at Norsk Pressefor-

bund oppretter ett seriøst nettsted der alle interesserte kan delta i en offentlig samtale om journalistikk og mediespørsmål. Her kunne redaktører, journalister, forskere, mediestudenter og -lærere, politikere, informasjonsmedarbeidere, konserndirektører, medieofre og det brede, interesserte publikum møtes til samtale. Ambisjonen er å legge opp til debatter om aktuelle saker og om mer prinsipielle, overordnete spørsmål. Personvernkommisjonen mener at arbeidet med å forbedre pressens yrkesetiske retningslinjer og dermed også personvernet vil bli styrket gjennom en bredere mediedebatt, der også andre stemmer enn profesjonelle mediefolk slipper til. Kommisjonen vil derfor oppfordre Norsk Presseforbund til å følge opp dette forslaget.

13.2.4.3 Statlig medieombud?

I boken *Norge – en diagnose* (red. Knut Olav Åmås) drøfter Ingjald Ørbeck Sørheim den norske pressen i essayet «Mediemakt uten motmakt, medieofre uten vern». Sørheim mener at det i Norge ikke finnes noen reell motmakt til pressen, og at uten egne talspersoner står enkeltborgerne svakt i konflikter med mediene.

Andre profilerte samfunnsdebattanter, som Terje Angelshaug (2008), Carl Erik Grimstad (2008) og Dag Solstad har sluttet seg til kritikken av pressen og da særlig «ønsket om å tjene mest mulig penger på å tilfredsstille publikums nysgjerrighet om andre menneskers privatliv» (Solstad 2008).

Personvernkommisjonen mener det er all grunn til å være skeptisk til både medienes makt og visse praksiser i mediene, særlig når det gjelder kriminaljournalistikk og kjendisjournalistikk, fordi det er særlig på disse områdene at personvernet utfordres.

Det må hele tiden føres en løpende diskusjon, både innenfor og utenfor medienes rekker, om roller, ansvar og normer. Men alt kan neppe reguleres i lovs form, og derfor mener Personvernkommisjonen at det er fornuftig at det finnes egne organer som forvalter en felles forståelse og håndheving av hva som er *yrkesetisk* forsvarlig medieadferd.

Personvernkommisjonen mener at PFU, slik dette er organisert som en del av Norsk Presseforbund, først og fremst er et redskap for pressen selv til å øke bevisstheten og forståelsen av en god etisk standard.

Personvernkommisjonen har observert at den engelske avisa The Guardian, siden 1998, og den danske avisen Politiken, siden 2001, har hatt en egen stilling med betegnelsene «reader's editor» og «lesernes redaktør». Denne redaktøren skal fungere som lesernes representant i redaksjonen. Jobben er å sikre at alle henvendelser og klager om det redaksjonelle innhold blir hørt, undersøkt, besvart og formidlet til rette vedkommende. I Norge har Bergens Tidende en lignende stilling i sin redaksjon med betegnelsen «leserombud». Personvernkommisjonen mener at et slikt leserombud både kan bidra til å lette arbeidet med å nå fram til redaksjonen med klager på presseetiske overtramp, bidra til større oppmerksomhet omkring presseetiske spørsmål internt i redaksjonen og synliggjøre klagemulighetene for publikum. På den annen side kan en slik egen stilling også bidra til å pulverisere det ansvaret for etiske overtramp som i dag hviler på ansvarlig redaktør. Personvernkommisjonen vil derfor ikke ta stilling verken for eller i mot at norske media har egne «leserombud», men synes det er nyttig at det i Bergens Tidene høstes erfaringer med en slik ordning.

13.2.5 Avtaler

Tilbydere av ulike nettbaserte informasjonstjenester, med Facebook og Google som de fremste eksemplene, forsøker å regulere personvernfeltet gjennom eksplisitte avtaler[2] som inngås mellom selskapene og de som bruker selskapenes tjenester.

Disse avtalene inngås gjerne gjennom såkalt «click-wrap» (samtykke, samt at vilkårene i avtalen er gjennomlest og forstått, bekreftes ved at brukeren «klikker» med en dertil egnet innretning på en virtuell «knapp»), eller gjennom implisitt samtykke (en plakat på et passende sted informerer brukeren om at ved å gjøre bruk av tjenesten tilkjennegir brukeren at han samtykker i bestemte vilkår).

Disse avtalene er ofte urimelige sett fra brukerens ståsted. Som regel innebærer de blankoavskriving av ulike rettigheter, inklusive personvernrettigheter, og de inneholder klausuler som gir tjenesteyter rett til når som helst å endre avtalen. Etter Personvernkommisjonens oppfatning kan det stilles spørsmål ved om disse avtalene er gyldige, og vi vil oppfordre Forbrukerrådet til å gjøre en gjennomgang av avtalene knyttet til de mest populære tjenestene (eks.: Facebook, Gmail) for å vurdere lovligheten opp mot norsk

[2] Slike avtaler kan ikke erstatte preseptoriske (ufravikelige) lovregler.

lov, og hva som kan gjøres dersom disse avtalene strider mot norsk lov.

13.2.6 Allmennmoralen

Om vi trekker fra det som reguleres av alle de instrumentene og organene som vi så langt har omtalt, gjenstår det fortsatt et stort rom. Dette gjenværende rommet reguleres av det vi i mangel av et bedre begrep vil kalle for allmennmoralen eller «folkeskikken».

Begrepet refererer til den mengden av normer og verdier som regulerer mellommenneskelige relasjoner og vårt sosiale dagligliv. Dette er normer og verdier som stammer fra sed og skikk, og som vi mer eller mindre aksepterer fordi de inngår i vår oppdragelse og er en del av vår kulturarv.

Når det gjelder «nye media», som ikke driver med journalistikk, og som det ikke derfor er naturlig for PFU å forholde seg til, finnes det knapt noen allment aksepterte systematisk begrunnede etiske retningslinjer tilsvarende PFUs yrkesetiske retningslinjer.

Allmennmoralen/folkeskikken gjelder for disse mediene som for alle andre områder i samfunnet. Mobbing og andre former for uetisk adferd er imidlertid et voksende problem innenfor nettbaserte media (Hinduja og Patchin 2008), og det kan virke som om nettet er mindre regulert av det vi kaller vanlig folkeskikk enn når vi kommuniserer ansikt til ansikt.

Personvernkommisjonen mener at dette bør det gjøres noe med. Det vil styrke personvernet om det arbeides videre med å utarbeide og formidle gode etiske retningslinjer for disse mediene.

13.3 Medietyper og medieroller

Det mangfoldet som er oppstått i kjølvannet av digitalisering, konvergensutviklingen og den generelle utviklingen på kommunikasjonsområdet, har gitt oss nye media med ulike publiseringspraksiser. Enkelte av de nye mediene har arvet mye fra de «tradisjonelle» mediene. Mange nettaviser ligner for eksempel på papiraviser. De fylles med innhold som skapes av en profesjonell redaksjon og er styrt av en ansvarlig redaktør.

Imidlertid har de fleste nettaviser debattfora hvor avisens lesere kan slippe til med meningsytringer om aktuelle saker. I noen nettaviser behandles disse på samme måte som man behandler leserinnleggene i en papiravis. Det vil si at innlegg fra leserne gjennomgår en redaksjonell vurdering og redigering. Alle innlegg blir vurdert ut fra om det har interesse for leserne, har en form og et innhold som ikke bryter med norsk lov (eller Vær Varsom-plakaten). Dette gjøres *før* de blir synlig på nett.

I andre nettaviser publiseres alle debattinnlegg fortløpende, uten at de på forhånd gjennomgår en redaksjonell vurdering og redigering. Dette begrunnes blant annet med at nettmediet har ubegrenset med plass og at man derfor ikke trenger å avvise ytringer av plasshensyn, og at man ønsker å utnytte de mulighetene for hurtig og umiddelbar interaksjon som nettmediet gjør mulig.

Andre nettbaserte media skiller seg enda mer radikalt fra tradisjonelle media, ved at de utnytter de mulighetene som teknologien gir til å samle inn informasjon om sine brukere, og på det viset utfordrer de personvernet.

Gjennom såkalte «blogger» og «hjemmesider» har Internett gjort det mulig for enhver å bli sin egen utgiver, noen av disse har innhold hentet fra utgiverens privatliv, andre er mer journalistiske i sin utforming. Nye innretninger, og da særlig mobiltelefoner med innebygget videokamera og mulighet til videresending av multimediemeldinger, har bidratt ytterligere til å gjøre skillet mellom privatliv og offentlighet utydelig.

Nedenfor beskriver vi disse ulike medietypene og medierollene, og peker på utfordringer særlig disse mediene skaper for personvern og personopplysningsvern.

13.3.1 Redigerte media

Felles for de «tradisjonelle» massemediene er at de er *redigert,* og at de har en ansvarlig *redaktør*. Redaktøren har både ansvaret for hvordan produksjonen organiseres, og som vi har sett kan redaktøren både strafferettslig og sivilrettslig stilles til ansvar for det ferdige produktet. I vår videre vurdering slår vi alle tradisjonelle massemedia sammen i en kategori som blir kalt «redigerte» massemedia.

I redigerte massemedia legges det til grunn at redaktøren har utformet en redaksjonell linje som er kjent av medarbeiderne, og som blant annet setter grenser for hvordan mediet forholder seg til stoff som krenker eller utfordrer personvernet.

13.3.2 Etter-redigerte media

Mange nettaviser har, blant annet på grunn av den store mengden innlegg, ingen redaksjonell vurde-

ring på forhånd av lesernes innlegg. I stedet tar disse nettavisene brukere og lesere til hjelp, ved at de kan varsle om «upassende innlegg». Den redaksjonelle kontrollen består av at redaksjonen griper inn i etterkant, og redigerer eller fjerner upassende innlegg fra nettet i den utstrekning man gjennom varsling eller på annen måte blir kjent med at slike foreligger. Denne redaksjonelle praksisen har vi valgt å kalle «etter-redigert».

Ansvarlig redaktør for nettutgaven av svenske Aftonbladet, Kalle Jungkvist, beskriver på denne måten forholdet mellom de tradisjonelle mediene og de nye nettmediene som debattarena:

> «Debatten i traditionella medier är i grunden förbehållen ett fåtal. På ledar-, kultur- och debattsidor förs en elitdebatt. På insändarsidorna väljer en redaktör ut några få inlägg som skrivs om och kortas ner. I grunden handlar det om envägskommunikation, tidningen som talar till läsarna – inte om ett brett samtal och meningsutbyte mellan läsare. Nätet har skapat helt nya möjligheter för människor att diskutera, kritisera och driva opinion. Bara på aftonbladet.se har vi dagligen publicerat i snitt 1 500 inlägg, ända upp till 6 000 om debatten varit riktigt het. (Jungkvist 2002)»

Fra et personvernperspektiv kan slik etter-redigering være problematisk. I etter-redigerte media er det i prinsippet ingen ting som hindrer en krenkelse i å bli offentlig. Selv om den fjernes i etterkant kan skaden alt ha skjedd. Gjør man det mulig å ytre seg i et slikt medium uten noen form for registrering, vil det også være mulig fremsette slike krenkelser anonymt eller pseudonymt.

Generalsekretær Nils E. Øy i Norsk Redaktørforening opplyste på Personvernkommisjonens mediekonferanse i februar 2008 at nær 40 % av foreningens bedriftsmedlemmer forhåndsredigerer alt brukerskapt innhold, og at ca. 65 % av de øvrige krever registrering, for eksempel e-post eller mobilnummer. Det innebærer at ca. 21 % av Norsk Redaktørforenings bedriftsmedlemmer verken forhåndsredigerer eller krever registrering.

13.3.3 Media som samler brukerinformasjon

Mens kommunikasjonen mellom «tradisjonelle» media og publikum i det alt vesentlige foregår enveis (fra mediet og til publikum), utnytter mange av de «nye» mediene den egenskapen at nettverksbasert kommunikasjon fungerer like godt begge veier.

En slik toveiskommunikasjon åpner blant annet opp for en bredere dialog, slik ansvarlig redaktør for nettutgaven av svenske Aftonbladet, Kalle Jungkvist beskriver ovenfor, men det åpner også opp for at mediet, med eller uten publikums vitende og vilje, kan hente inn og lagre de elektroniske sporene som oppstår som en bivirkning av at publikum bruker et elektronisk medium.

Som et eksempel på det siste vil vi vise til praksisene til selskapene Google og Facebook.

Selskapet Google dominerer markedet for søk etter informasjon på Internett, med en markedsandel i Norge anslått til 80-90 % (Dagens Næringsliv 2007). Det er åpenbart at forretningsideen bak Google ikke er å selge tjenesten «søk» (derfor er det gratis å søke). I stedet genererer Google inntekter for sine eiere ved å selge reklame gjennom et eget system for nettreklame. Reklamen «spisses» inn mot den enkelte bruker av tjenesten ved å samle inn personopplysninger som bearbeides og foredles på ulike måter. Når du gjør et søk på Google, lagrer selskapet følgende informasjon:

1. Din datamaskins unike ip-adresse.
2. Nummeret på informasjonskapselen Google har lagret på din maskin.[3]
3. Hvilke av søkeresultatene du klikker på.
4. Ordet eller uttrykket du søkte på.
5. Hvilken nettadresse du søkte fra.
6. Tidspunkt og dato.
7. Hvilken nettleser du bruker og hvilket operativsystem PC-en din har.

Google lagret tidligere slik informasjon i 2 år. Etter påtrykk fra personvernmyndigheter i EU anonymiserer Google nå ip-adresser etter 9 måneder (Fleischer et al. 2008).

I tillegg til individuelt tilpassede annonseplasseringer, er det antatt av mange at Google også selger ulike former for «business intelligence», basert på de data selskapet samler inn og foredler. Det som leveres ut er imidlertid neppe personopplysninger, men aggregerte data om ulike populasjoner.

I tillegg til den informasjonen Google samler inn i samband med søk, har Google for eksempel tilgang til samtlige sendte og mottatte e-post-meldinger til brukere av tjenesten Gmail.

Nok en redaksjonell praksis finner vi på ulike sosiale nettsteder eller nettsamfunn som bygges opp rundt foredling av ulike former for brukerskapt innhold, slik som Facebook, Flickr, YouTu-

[3] Microsoft Internet Explorer versjon 8 har en egen modus (InPrivate) som automatisk vil slette slike informasjonskapsler når sesjonen avsluttes

be, MySpace, Blink (Dagbladet), Nettby (VG) og Underskog.

I likhet med nettavisens brukerforum stammer innholdet på slike nettsteder fra brukerne selv. Hos noen innebærer dette rett og slett bare at brukerne tilbys en nettflate der de kan realisere eget innhold. Nettstedet rolle er dels å gjøre brukernes innhold attraktivt og synlig for et så stort publikum som mulig gjennom å pakke det sammen med en infrastruktur for søk og navigasjon, dels å tjene penger på dette innholdet gjennom salg av tilknyttet reklame. Men enkelte sosiale nettsteder går enda lenger. Det mest ekstreme eksemplet i dag er Facebook.

Facebook ble startet i 2004 av Mark Zuckerberg da han var student på Harvard og har (juni 2008) cirka 79 millioner medlemmer verden over. Ifølge europasjef Blake Chandlee i McCann Worldgroup er hver fjerde nordmann (nesten 1,2 millioner) medlem av Facebook (Dagens Næringsliv 2008). Hvert medlem lager en profil for seg selv, knytter til seg venner, og kan dele sine aktiviteter med disse vennene. Facebook er gratis, men tjener penger på annonser.

Facebook forutsetter at man oppretter en profil på nettstedet. For å opprette denne profilen oppfordres man til å oppgi en rekke personopplysninger. Noen av disse personopplysningene (eksempelvis om politisk oppfatning og livssyn) tilhører kategorien sensitive opplysninger som det i Norge forutsettes at behandlingsansvarlige i utgangspunktet har konsesjon fra Datatilsynet for å behandle.[4]

I likhet med andre sosiale nettsteder tilbyr Facebook sine medlemmer ulike publiseringsflater der de kan legge ut tekster, fotografier, videoer, og lignende. Men i tillegg *overvåker* Facebook sine brukeres adferd, og registrerer alle endringer. Hvem som knytter vennskap med hvem, hvem som gir hverandre presanger, hvem som endrer sivil status, osv.

Videre overvåker Facebook transaksjoner som skjer på samarbeidende nettsteder gjennom et eget system som går under navnet *Beacon*. Kjøper man for eksempel forlovelsesring i en nettbutikk knyttet til systemet, kan dette bli rapportert til Facebook og registrert. I sin opprinnelige utforming var systemet slik at hele denne strømmen av små og store begivenheter og handlinger umiddelbart ble publisert på Facebook som «nyheter» om den person det gjelder. Etter at systemet kom under sterk kritikk fra personvern-forkjempere ble det endret slik at en «nyhet» ikke blir publisert før publiseringen er godtatt av den person den angår. Systemet ble i tillegg endret slik at det er mulig å reservere seg fra det. Det bør videre nevnes at disse høyst personlige «nyhetene» ikke er offentlig tilgjengelig, men kun synlig for alle dem som tilhører vennskapskretsen til den person det gjelder (slik en slik krets defineres av Facebook).

På mange måter kan Facebook betraktes som en slags informasjonskanal som handler om dine Facebook-venners små og store gjøremål. Ved at nyhetsstrømmen avgrenses til en lukket krets[5], kan det stilles spørsmål ved hvorvidt nettsamfunn av type Facebook virkelig er et massemedium. Vi har imidlertid valgt å ta det med her, blant annet fordi vi tror at denne typen hybridløsninger, der grensene mellom det offentlige og private viskes ut, er en forsmak på den typen media vi vil møte i fremtiden.

Av mangel på et bedre begrep har vi valgt å kalle denne type media for «web 2.0», fordi «web 2.0» er det ord man gjerne finner i litteraturen når noen har behov for å karakterisere denne typen medium og redaksjonell praksis. Det er særlig selskapet O'Reilly Media som har bidratt til å gjøre dette begrepet kjent. Siden 2004 har det vært holdt årlige konferanser med «web 2.0» som tema (O'Reilly 2005).

Det er neppe tvil om at selskaper som samler inn og lagrer store mengder personopplysninger, ved bruk av vanlige teknikker for strategisk informasjonsanalyse, kan hente ut en rekke personopplysninger fra den informasjonen de har i sin besittelse, inklusive sensitive sådanne.

Den innsamlingen og systematiseringen av personopplysninger som gjøres av denne typen media, utfordrer på mange måter nasjonal lovgiving på personopplysningsområdet. Datatilsynet har uttalt at virksomheten til Facebook ikke er underlagt kravene i den norske personopplysningsloven eller annen tilsvarende europeisk lovgivning, ettersom selskapet (som er ansvarlig for behandlingen av personopplysningene, jf. personopplysningsloven § 2 nr. 4) er etablert utenfor Norge og EØS-området (VGnett 2007). Personvernkommisjonen stiller seg spørrende til om denne uttalelsen rettslig sett er riktig. Facebook

[4] Man kan imidlertid la disse feltene i Facebook-profilen være blanke, og man kan selvsagt også lyve.

[5] Ordet «venn» i Facebook har imidlertid en langt videre betydning enn det folk vanligvis forbinder med begrepet. En undersøkelse gjort av datasikkerhetsfirmaet Sophos (2007) viser for eksempel at 41 % av Facebook-brukerne er villig til å innlemme en fiktiv person i vennekretsen.

vil i prinsippet rammes av norsk lov dersom selskapet benytter seg av «hjelpemidler» lokalisert i Norge. Dette følger av personopplysningsloven § 4 annet ledd. I følge lovens forarbeider omfatter begrepet «hjelpemidler» bl.a. «datamaskiner og -terminaler, telenett og intervjuskjemaer» (Ot.prp. nr. 92, (1998-99), s. 106). Det kan godt argumenteres for at Facebook benytter seg av slike hjelpemidler i samhandlingen med Facebook-brukere som oppholder seg i Norge, og som følgelig bruker datautstyr som er lokalisert i Norge. Argumentet gjelder også dersom Facebook lagrer informasjonskapsler («cookies») på harddiskene til disse brukerne (jf. også Art 29 WP 2002, s. 11). Problemet er imidlertid at det er svært vanskelig for norske myndigheter å håndheve loven overfor utenlandskbaserte aktører som Facebook. Det finnes likevel eksempler på at nasjonale myndigheter i samband med andre lands myndigheter har lykkes i å få visse utenlandsbaserte aktører til å endre praksis i personvernvennlig retning, jf. Googles beslutning (referert ovenfor) om å anonymisere ip-adresser etter 9 måneder.

13.3.4 Egenpubliserte media

Internettbaserte media har også gjort det enkelt og billig for privatpersoner å bli sin egen utgiver. Det kan skje enten gjennom en hjemmeside, eller gjennom en «blogg» (forkortelse for «web-logg» – en dagboklignende nettpublikasjon). Begge kan lages med et enkelt publiseringsverktøy som kan anvendes av alle som vet hvordan man kobler seg på nett. Noen av disse selvredigerte nettstedene er til forveksling lik nettsteder hvor det står en profesjonell redaksjon bak, andre er av helt privat karakter. De fleste av disse nettstedene har en svært begrenset publikum. En observasjon som gjerne tillegges Andy Warhol er at i fremtiden kan alle nyte 15 minutters berømmelse, og i samme ånd er det observert at på Internett kan alle nyte berømmelse for 15 personer. Men selv om den faktiske leserkrets er begrenset, er alt som publiseres på Verdensveven tilgjengelig for enhver som er knyttet til nettet. Derfor er heller ikke dette publikasjoner som befinner seg i den private sfære. Vi kaller den redaksjonelle praksis som ligger bak blogger og hjemmesider for «egenpublisert».

Disse egne mediene utfordrer personvernet ved at personene som står bak dem ofte har begrenset kunnskap om presseetiske spørsmål. For eksempel la en profilert blogger og høyrepolitiker i 2006 ut diverse nakenbilder av et «kjendispar» på sin blogg, tilsynelatende uten å være klar over at dette var ulovlig (Grimstad 2008, s. 18).

I noen tilfelle er dessuten utgiver av slike egenpubliserte media umyndig og kan derfor ikke stilles til rettslig ansvar for ytringer som krenker andres personvern.

13.3.5 «Media» i den private sfære

Brev sendt på tradisjonell måte gjennom posten og samtaler på fasttelefon betraktes ikke som massemedia, og er følgelig unntatt fra medieregulering.

Når det gjelder deres elektroniske motstykker, e-post og mobile telefontjenester med tilhørende meldingstjenester (SMS, MMS, samt mobile kringkastingstjenester for videofilm som DVB-H), er ikke skillet like klart. En e-post-liste kan ha tusenvis av abonnenter, og kan dermed leses av flere personer enn en liten lokalavis eller tidsskrift. Gjennom mobile meldingstjenester sprer innhold seg raskt og effektivt. Siden slik spredning skjer i den private sfære, er den vanskelig å kvantifisere. Det finnes derfor ingen oversikt over hvor mange mobiltelefonbrukere som mottok MMS-meldinger med svært private fotografier stjålet fra en kjent norsk skuespiller i oktober 2006, men det er sannsynligvis snakk om flere tusen.

Det er videre utviklet nye teknikker for spredning av innhold over Internett som har fått betegnelsen «P2P» (*peer-to-peer* eller *person-til-person*) som gjør det mulig for enkeltpersoner å «dele» innhold ved å sende det fra person til person. Takket være teknikken kan slik personlig «deling» skje i svært stor skala. Den vanligste bruken av disse teknikkene er spredning av opphavsrettsbeskyttet film og musikk.

Et signal om at det blir stadig vanskeligere å avgjøre om denne typen formidling tilhører den private eller den offentlige sfære, er at kringkastingsselskaper som BBC og NRK har begynt å eksperimentere med slik P2P-teknologi (Solheim 2008) til å formidle regulært programmateriale over nett.

Personvernkommisjonen er derfor kommet til at også denne typen formidling i visse tilfelle kan regnes som massemedia. Vi tar den derfor med i vår oversikt over medietyper, under betegnelsen «person-til-person».

Flere bestemmelser som er ment å verne om privatlivets fred forutsetter en offentliggjøring eller offentlig meddelelse, og det kan stilles spørsmål ved om P2P faller inn under disse kriteriene.

Personvernkommisjonen mener at spørsmålet bør avklares bedre, og at det bør vurderes hvordan personvernet kan styrkes i forhold til spredning av personvernkrenkelser ved hjelp av P2P-teknologi.

13.3.6 Medietyper: Oppsummering

Vi har ovenfor foretatt en inndeling av mediene i fem ulike medietyper:

1. *Redigert*. Massemedia som er underlagt tradisjonell redaksjonell gjennomgang og vurdering og redigering.
2. *Etter-redigert*. Brukerskapt innhold som ikke forhåndsredigeres, og som blir publisert på ett nettsted der det finnes en redaksjon som også publiserer redaksjonelt innhold som forhåndsredigeres.
3. *Web 2.0*. Sosiale nettsteder hvor det finnes en teknisk tilrettelegger som sørger for å tilrettelegge publiseringsflater som kan fylles med brukerskapt innhold, som gjerne analyseres med tanke på spisset markedsføring og lignende. Her finnes det også innhold som genereres automatisk basert på brukernes aktiviteter, men uten noen egentlig redaksjon.
4. *Egenpublisert*. Publikasjoner der privatpersoner opptrer som sin egen utgiver. Eksempler: blogger, «private» hjemmesider.
5. *Person-til-person*. Moderne elektronisk kommunikasjon som i utgangspunktet finner sted fra person til person, men som gir mulighet til å spre digitalt innhold til en så stor krets at det ligner et massemedium.

13.3.7 Roller

For å kunne skape gode betingelser for personvern i mediene trenger vi å forstå hvem det er som er i posisjon til å krenke personvernet, eller til å forhindre eller redusere skadeomfanget i samband med krenkelser. I samband med at en ytring ytres og formidles til en mottaker er mange ledd involvert. Vi mener at vi kan identifisere følgende seks roller i formidlingskjeden:

1. Opprinnelig ytrer.
2. Redaktør.
3. Utgiver.
4. Tjenesteyter (teknisk tilrettelegger).
5. Ren videreformidler.
6. Mottaker (av ytringen, dvs. leser, lytter, seer).

   Og til sist har vi (dersom ytringen handler om minst én person):

7. Den omtalte (den eller de personer som ytringen taler om).

I mediesammenheng er *opprinnelig ytrer* den person som opprinnelig fremsetter en ytring som formidles gjennom et massemedium. Ytringen som fremsettes kan enten formidles til publikum i fullstendig uredigert form, noe som typisk vil være tilfelle i ulike typer uredigerte media. Eller ytringen kan formidles til publikum etter å ha gått gjennom en redaksjonell prosess der ytringen kan bearbeides på ulike måter, fortrinnsvis for å gjøre budskapet til den opprinnelige ytrer tydeligere og enklere for publikum å oppfatte. Den redaksjonelle bearbeidelsen kan være så minimal som en ren sortering og kvalitetssikring (der redaksjonen velger ut de ytringer som skal komme på trykk og kasserer resten), den kan være en språklig bearbeidelse (språkvask), eller den kan være mer inngripende, i form av gjenfortelling, parafrasering eller referat. Avhengig av denne prosessen, eller fravær av den, fremstår opprinnelig ytrer i det ferdige produktet i en bestemt rolle, som, for eksempel, blogger, essayist, leserbrevskribent, kilde, eller intervjuobjekt.

Når det gjelder rollen som *redaktør* så følger denne i forhold til forhåndsredigerte media av straffelovens definisjon («Ved redaktør […] forstås […] den som treffer avgjørelse om skriftets innhold», jf. straffeloven § 436). Når det gjelder trykt skrift og kringkasting, er disse mediene dessuten pålagt å ha en ansvarlig redaktør og å opplyse om hvem dette er (jf. straffeloven § 429). Men for mange av de «nye» mediene, og i særdeleshet media som er tuftet på brukerskapt innhold uten noen form for forhåndsredigering, er det ofte uklart hvor det redaksjonelle ansvaret befinner seg, og dermed også uklart hvem man skal henvende seg til dersom et slikt medium formidler en ytring som krenker personvernet.

En *utgiver* er den personen eller det selskap som utgir et medium, og representerer eierne av et medium. Gjennom Redaktør-plakaten og den nye «Lov om redaksjonell fridom i media» (se avsnitt 13.2.1) er det slått fast at det er redaktøren og ikke utgiver som skal lede den redaksjonelle virksomheten og treffe avgjørelser i redaksjonelle spørsmål innenfor rammen av grunnsynet og formålet virksomheten bygger på. Utgiver kan heller ikke instruere eller overprøve redaktøren i redaksjonelle spørsmål.

Vi har tidligere (avsnitt 2.1.1) drøftet definisjonen av *tjenesteyter* som en som yter informasjonssamfunnstjenester, og vil her bare minne om at

denne rollen finner vi definert i ehandelsloven § 1 annet ledd.

I tillegg til tjenesteyter, som yter informasjonssamfunnstjenester, snakkes det gjerne om en *ren videreformidler* av ytringer eller *rene overføringstjenester* («mere conduit»). For en slik tjenesteyter avskjæres ansvaret i ehandelsloven § 16. Paragrafen definerer et sett med krav for at tjenesteyter skal komme i denne kategorien (overføringen må ikke starte hos tjenesteyteren, tjenesteyteren kan ikke selv velge mottaker, og tjenesteyteren kan ikke selv bestemme eller endre det som overføres). I så fall, sier ehandelsloven, kan den som yter tjeneste ikke pålegges noe strafferettslig eller erstatningsrettslig ansvar for det som formidles.

Det siste leddet i formidlingskjeden er ytringens *mottaker*. Her vil vi bare slå fast at mottaker ikke har noe ansvar for ulovlige ytringer, bortsett fra dersom han aktivt inntar rollen som videreformidler.

Når mediene krenker personvernet til noen er det i første rekke *den omtalte* som har ansvar for at forholdet påtales. Dette kan for eksempel skje ved å anmelde forholdet til politiet, ved å ta ut sivilt søksmål, eller ved å klage krenkelsen inn for et forvaltningsorgan eller selvreguleringsorgan.

13.3.8 Retten til anonymitet

I forbindelse med ansvarsplassering for ytringer er også identitet (eller snarere – fravær av identitet) viktig. Hvordan kan noen gjøres ansvarlig for en rettsstridig ytring, dersom man ikke vet hvem vedkommende er?

I dag finnes det både kommersielle tjenester og ymse gratistjenester som utvikles av tilhengere av et sterkt personvern, som har som formål å gjøre det mulig å være anonym på Internett.

Retten til anonymet er imidlertid omstridt. Skribenten Bernd Graff i Süddeutsche Zeitung mener at mulighetene nettet gir til anonym utskjelling og ryktespredning er ødeleggende for debatten: «[D]et vi ser er diskursens død, drevet av indignasjon … brukergenerert innhold slett ikke sjelden er tapergenerert innhold » (Wiese 2007).

Noen benytter seg bevisst av nettets anonymitet til å begå lovbrudd. Av den grunn foreslo daværende leder for Økokrims datakrimavdeling at det ikke bør være lov for tjenesteytere å tilby tjenester der det er mulig å operere anonymt (Sunde 2000, s. 287).

Retten til å ytre seg anonymt har imidlertid lange tradisjoner i Norge. Allerede året etter at Struensee opphevet forhåndssensuren i 1770 ble skjult identitet for forfattere av trykt skrift akseptert. Begrunnelsen, som det fremgår av nedenstående sitat fra P.K. Gaarders klassiske verk om Grunnloven (Gaarder 1845), var at retten til å operere med skjult identitet var en naturlig følge av ytringsfriheten og en nødvendig forutsetning for at folk kunne varsle om kritikkverdige forhold gjennom mediene uten at det førte til represalier:

> «Uagtet imidlertid Ordene i Paragrafen efter det forananførede neppe kunde paaberaapes som hjemlende Anonymitet, er det dog forlængst erkjent hos fri Nationer, at et Forbud herimod ligesaalidt er nødvendigt som gavnligt, idet ved samme et Baand lægges paa den fri Ytringsret, der hindrer den almindelige Benyttelse af denne gjennem Pressen, som Opnaaelsen af Trykfrihetens Hensigt fordrer og Grundloven tilsigtet. Det var derfor vistnok med fuld Føie man allerede strax ved dennes Indførelse ansaa at det ældre gældende Forbud i Frdn. af 27de Septbr. 1799 imod Anonymitet for umiddelbart hævet. »

Også i vår tid er man oppmerksom på dette. I Europarådets erklæring om kommunikasjonsfrihet på nett (Erklæring om kommunikasjonsfrihet på Internett, vedtak i Ministerkomiteen 28. mai 2003) står det:

> «Prinsipp 7: Anonymitet: For å sikre vern mot direktekoblet overvåking og for å fremme friheten til å uttrykke informasjon og ideer bør medlemsstatene respektere Internett-brukernes ønske om å ikke avsløre sin identitet.»

I vår egen tid ser vi at offer for overgrep og folk som er rammet av bestemte sykdommer finner sammen i ulike nettmedia og kan dele sine problemer med likesinnede og terapeuter. Også varslere har behov for å kunne varsle anonymt. I slike sammenhenger er det opplagt at retten til å være anonym er viktig for personvernet.

Etter Personvernkommisjonens oppfatning er retten til å ytre seg anonymt både en personvernrettighet og en rettighet knyttet til ytringsfrihet, og derfor særdeles viktig å bevare. Samtidig er det ingen tvil om at retten til å være anonym også utfordrer personvernet, blant annet ved at ærekrenkelser og brudd på privatlivets fred spres anonymt på Internett.

Også på Struensees tid var man oppmerksom på dette dilemmaet, og det ble den gang løst på den måte at dersom den opprinnelig ytrer opptrer anonymt, må den omtalte gis et annet ansvarssubjekt å forholde seg til (jf. Røhnebæk 2002, s. 511).

Derfor ble det bestemt at enhver trykksak måtte bringe navn på enten forfatteren eller boktrykkeren. Dersom en forfatter i 1771 ønsket å ytre seg anonymt, måtte han altså finne en boktrykker som var villig til å sette sitt navn og rykte i pant for ytringene. Ideen fra Struensees tid om at minst én ansvarlig person for en ytring skal kunne identifiseres, er prinsippet som ligger bak, så vel det særlige redaktøransvaret som kildevernet.

Som vi tidligere har nevnt, er det uklart i hvilken grad det særlige redaktøransvaret gjelder for andre media enn trykt skrift og kringkasting. Personvernkommisjonen mener at det er viktig for personvern i mediene at den omtalte til enhver tid har et ansvarssubjekt som kan kontaktes for å få løst personvernkrenkelser i minnelighet, eller som kan gjøre strafferettslig eller sivilrettslig ansvarlig dersom krenkelsen ikke kan løses på annen måte.

13.4 Skattelister og pliktavlevering av elektronisk materiale

I dette avsnittet presenterer vi to områder som vedrører media og personvern, som ikke henger sammen med medietyper og medieroller.

Det første punktet – offentliggjøring av skattelistene – har vi valgt å omtale i denne delen av rapporten fordi det først og fremst er medienes bruk av skattelistene som reiser de personvernmessige problemstillingene.

Det andre punktet – pliktavlevering av elektronisk materiale – behandles i kapittelet om personvern og media fordi pliktavlevering av nettpublikasjoner etter kommisjonens vurdering reiser særlige problemer sett fra et personvernsynspunkt.

13.4.1 Offentliggjøring av skattelistene

Åpenhet omkring og offentliggjøring av skattelister med opplysninger om hva den enkelte tjener og betaler i skatt har tradisjoner helt tilbake til midten av 1800 tallet.

Slik offentliggjøring anses som viktig for den offentlige debatten om hvordan skattesystemet fungerer, og blir sett på som en forutsetning for at folk skal ha tillit til at skattesystemet er rettferdig. Her kan man finne ut hvor mye enkeltpersoner og ulike grupper bidrar med til fellesskapet. Et argument for offentliggjøring har vært at åpenhet rundt skattelistene virker forebyggende i forhold til svart arbeid, korrupsjon og annen økonomisk kriminalitet. Mediene bruker denne informasjonen både i sin kritiske journalistikk og til mer underholdningspregede oppslag, for eksempel «på topp»- og «på bunn»-lister med fokus på kjendispersoner. Media tilbyr også søk i skattelistene i forhold til enkeltpersoners inntektsforhold, uten at dette har et utelukkende journalistisk motiv.

Enkelte har pekt på at offentliggjøring av skattelistene krenker personopplysningsvernet, både fordi opplysninger av økonomisk karakter er noe vi anser som personlig og på grunn av misbrukspotensialet. Fordi listene viser nettotall, gir de heller ikke nødvendigvis et riktig bilde av den enkeltes inntekts- og formuesforhold. Det har blitt hevdet at tilgangen på listene har gjort det enklere for forbrytere å plukke ut ofre med store inntekter og/eller formuer og at det åpnes for sammenstilling og massedistribusjon av personopplysninger.

Offentliggjøring av skattelister har hjemmel i ligningsloven § 8-8. Listene inneholder følgende opplysninger om skattebetalerne: navn, fødselsår, poststed og postnummer, skattekommune, nettoinntekt, nettoformue og utliknet skatt. Skattelistene gjøres tilgjenglige for søk på Skatteetatens nettsider i tre uker, men opplysningene fremkommer kun etter søk på identifiserbare personer.

I henhold til ligningsloven § 8-8, nr. 3, 4. ledd kan pressen få fullstendige skattelister i elektronisk form. Det er særlig denne formen for tilgjengeliggjøring som har vært gjenstand for debatt, og reglene har vært endret flere ganger. Blant annet skjerpet man reglene for offentliggjøring i 2004. Da ble listene gjort tilgjengelige for enkeltsøk i kun tre uker etter offentliggjøringen. I 2007 vedtok imidlertid Stortinget at pressen igjen kunne bestille skattelistene elektronisk, blant annet begrunnet i et ønske om å styrke den kritiske debatten rundt skattesystemet.

I Skatteetatens retningslinjer for offentliggjøring av skattelister (Skatteetaten 2004), er det presisert at bruk av skattelisteopplysninger skal følge personopplysningslovens regler. Når pressen bruker opplysningene som ledd i journalistisk virksomhet, vil imidlertid personopplysningsloven bare i svært begrenset grad komme til anvendelse, jf. § 7. Dette er begrunnet i hensynet til ytringsfriheten.

Selv om offentliggjøring av skattelister har hjemmel i lov, er det grunn til å diskutere om dagens praksis er i samsvar med overordnede personvernrettslige prinsipper som blant annet kan utledes av EMK og EUs personverndirektiv.

Som nevnt tidligere i dette kapittelet, er staten, i henhold til EMK artikkel 8 (1), pliktig til å ha lo-

ver som verner privatlivets fred. Inngrep i denne retten må oppfylle vilkårene i artikkel 8 (2), det vil si at dersom offentliggjøring av skattelister medfører et inngrep i retten til respekt for privatliv, må inngrepet være hjemlet i lov og være nødvendig i et demokratisk samfunn. Offentliggjøringen må anses som et inngrep i privatlivet (se like nedenfor) og har lovhjemmel. Men det må likevel vurderes om inngrepet har et legitimt formål, det vil si om det kan begrunnes i et tungtveiende samfunnsmessig behov, og om inngrepet i privatlivet er proporsjonalt i forhold til det som anføres å være formålet med publiseringen.

Hvorvidt offentliggjøring av skattelistene utgjør et inngrep etter EMK artikkel 8 (1), har ikke blitt direkte besvart av Den europeiske menneskerettighetsdomstol. Den Europeiske menneskerettighetskommisjonen[6] har riktignok uttalt i saken *Lundvall mot Sverige* (dom 1985-12-11) at offentliggjøring av skatteopplysninger i Sverige den gang utgjorde et inngrep «of a minor nature», men at inngrepet var i samsvar med vilkårene i artikkel 8 (2).

Denne avgjørelsen har imidlertid begrenset betydning ved en vurdering av praksisen i Norge, da den tar for seg en situasjon som er svært annerledes enn våre tidsubegrensede nettbaserte søkemuligheter. EMD er heller ikke bundet av den daværende kommisjonens avgjørelser. Med tanke på at permanente søkemuligheter i skatteopplysninger må anses for å utgjøre en større personvernmessig ulempe enn den offentliggjøringen som fant sted i Sverige på midten av 1980-tallet, kan imidlertid den tidligere kommisjonens avgjørelse tas til inntekt for at dagens offentliggjøring av slike opplysninger på Internett må anses om et inngrep i privatlivets fred. I lys av senere praksis fra EMD, der ulike former for registrering og/eller spredning av personopplysninger gjentatte ganger er blitt ansett som inngrep i rettighetene etter artikkel 8 (1) (se om dette i kapittel 6.1.3), kan det stilles spørsmål ved om dagens praksis i Norge må betraktes som et inngrep som rammes av artikkel 8 (1).

Det er også verdt å merke seg at EF-domstolen i Rechnungshof-saken og den Østerrikske forfatningsdomstol i forhold til samme sak (se kapittel 6.2.4), la til grunn at offentliggjøring av inntektsopplysninger for navngitte arbeidstakere i visse offentlige organer som ledd i revisjonsvirksomhet hos den Østerrikske Riksrevisjon, utgjorde et inngrep etter artikkel 8 (1). EF-domstolen fant at lovligheten av en slik offentliggjøring i det vesentlige beror på en vurdering av hvorvidt offentliggjøringen kan anses som et *forholdsmessig* (*proportionate*) inngrep. Den østerrikske forfatningsdomstol konkluderte deretter med at Riksrevisjonens praksis ikke var i samsvar med proporsjonalitetskriteriet (jf. dom av 28. november 2003; omtalt bl.a. i Bygrave 2008).

Det er ikke tvil om at offentliggjøringen av skattelister slik det i dag praktiseres utfordrer sentrale personvernprinsipper. Det kan blant annet stilles spørsmål ved om pressens vide tilgang til og tilrettelegging for bruk av skattelistene for ren «underholdning», er i samsvar med formålet som begrunner publisering, nemlig å kontrollere likebehandling og skape debatt rundt skattesystemet. Pressens rolle i denne samfunnsdebatten kan ivaretas ved at media får bruke opplysningene som en alminnelig kilde, men at man setter restriksjoner i forhold til at hele skattelisten gjøres søkbar hos nettaviser i ubegrenset tid. Da ville behovet for offentlighet og debatt bli ivaretatt, men på en måte som er langt mindre inngripende for personvernet.

Man må også vurdere om det er nødvendig å publisere et så stort antall personopplysninger for å oppfylle formålet, og om opplysningene i det hele tatt er egnet til kontroll av misforhold og feil, da publiseringen skjer før klagefristen på ligningen er ute.

Personvernkommisjonen har ikke hatt anledning til å foreta en fullstendig vurdering av om dagens praksis knyttet til publisering av skattelistene er i samsvar med Norges internasjonale forpliktelser.

Det er kommisjonens oppfatning at en grundig vurdering av dagens praksis sett hen til internasjonale krav bør gjennomgås på nytt.

13.4.2 Pliktavlevering av elektronisk materiale

Etter lov om pliktavlevering av 9. juni 1939 skulle ett eksemplar av «alt hva det her i riket trykkes eller på annen måte mangfoldiggjøres av bok-, avis-, billed-, kart- eller notetrykkerier eller andre grafiske reproduksjonsanstalter», sendes til Universitetsbiblioteket i Oslo. Videre skulle ett eksemplar sendes til Universitetsbibliotekene i Bergen og Trondheim dersom disse institusjonene ba om det.

[6] Et organ som fram til 1998 gransket klager i henhold til EMK for å avgjøre om disse kunne prøves av EMD, men som deretter ble nedlagt

I 1989 ble loven endret, blant annet for å gjøre pliktavleveringen mediumuavhengig. Bakgrunnen for lovendringen er i Ot.prp. nr. 52 (1988-89) beskrevet slik:

> «Hovudgrunnane for å setja ei ny lov i staden for denne er at
> – medieutviklinga dei siste 50 åra har skapt ei rekkje nye informasjonsberarar for allment tilgjengeleg informasjon. Ei ny lov bør og femna om mikrofoner, edb-dokument, lydfestingar, fotografi, filmar, videogram og kringkasta materiale,
> – alle universitetsbiblioteka bør stillast meir på lik line, særleg for tradisjonelt bibliotekmateriale, samstundes som det og bør avleverast tryggingseksemplar og eksemplar for fjernlån.»

Pliktavleveringsloven § 4 bestemmer:

> «Dokument som er gjort tilgjengeleg for allmenta skal avleverast slik:
> – Dokument av papir eller papirliknande medium, mikroformer og fotografi i sju eksemplar.
> – Lydfesting, film, videogram, edb-dokument og kombinasjonar av desse dokumenttypane i to eksemplar.
> – Opptak av kringkastingsprogram i eitt eksemplar.»

Nasjonalbiblioteket ønsker, med utgangspunkt i denne bestemmelsen, å skape et stort permanent arkiv av digitalt innhold i Nasjonalbiblioteket.

Lovens formål er definert slik i § 1:

> «Føremålet med denne 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.»

Det er særlig pliktavlevering av elektroniske dokumenter kommisjonen har fokusert på og som må sies å reise særlige personvernutfordringer. Det er også grunn til å stille spørsmål ved om en slik omfattende pliktavlevering er tilstrekkelig gjennomtenkt og i tråd med lovgivers intensjon da loven ble vedtatt i 1989. Med «edb-dokumenter» er det mest sannsynlig at det siktes til databaser og CD-ROM. CD-ROM var lansert tre år tidligere under mottoet «the new papyrus» og ble av mange betraktet som det nye dokumentformatet (Maartmann-Moe 1991, s. 65). I 1989 var Internett ikke i bruk utenfor spesielle forskningsmiljøer, og Verdensveven eksisterte ikke.

Elektronisk pliktavlevering av dokumenter som befinner seg på den norske delen av Verdensveven skjer i dag ved at Nasjonalbiblioteket ved hjelp av såkalte søkeroboter som selv laster ned og arkiverer innhold. Da materialet som lastes ned også innebærer en digital behandling av personopplysninger, kreves det konsesjon av Datatilsynet for behandlingen, jf. personopplysningsloven § 33. Nasjonalbiblioteket har i dag en midlertidig konsesjon for dette.

Fordi Nasjonalbiblioteket selv laster ned materialet, trenger ikke utgiver foreta seg noe for at Nasjonalbiblioteket skal arkivere elektroniske dokumenter, og det er heller ikke mulig å reservere seg mot arkivering.

Intensjonen er å la arkivet omfatte samtlige norske nettsider, inklusive gamle versjoner av nettsider som for lengst er endret eller slettet av sine eiere. I samme arkiv lagrer Nasjonalbiblioteket samtlige meldinger som distribueres i den norske grenen av meldingssystemet *Usenet*. Både når det gjelder Verdensveven, og når det gjelder Usenet, finnes det en etablert industristandard (*Robot Exclusion Protocol*) for merking av sider, slik at disse sidene ikke skal registreres av søkemotorer og arkivtjenester. Alle de kjente kommersielle aktørene på nettet respekterer denne industristandarden. Google vil altså ikke gjøre en side søkbar dersom eieren av siden ved hjelp av denne standarden har markert at den ikke skal være søkbar, og The Internet Archive vil ikke arkivere en side dersom det er markert at siden ikke skal arkiveres. Nasjonalbiblioteket kjenner denne industristandarden, men har bestemt at de ikke akter å følge den.

Videre har Google, og sannsynligvis også flere av de andre søkemotorselskapene, utviklet rutiner som gjør det mulig raskt å fjerne midlertidig lagrede kopier og indekser. Dette er prosedyrer som kan benyttes i tilfeller der sensitive personopplysninger er lagt rettsstridig på Internett. Kommisjonen er ikke kjent med at Nasjonalbiblioteket har utviklet tilsvarende rutiner.

Personvernkommisjonen mener at 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.

Allerede i 1989 mente man at det ville være behov for å arbeide videre med utvalgskriterier og avgrensninger vedrørende avlevering av elektroniske dokumenter. Det sies i forarbeidene (Ot.prp. nr. 52 (1988-89)):

> «I røynda vil ein måtta gjera eit utval av edbdokument – tilgjengelege ved direktekopling – som skal avleverast. Ei altomfattande avlevering er neppe realistisk. Det må arbeidast vidare med utvalskriterium og avgrensingar. Fleire høyringsinstansar peikar på vanskane ved, og etterlyser retningsliner for, avlevering av databasar som vert kontinuerleg oppdaterte. Det lyt fastsetjast reglar om avleveringsintervall m.m. Generelt vil det gjelda at brigde av ein kumulativ karakter i mindre grad aktualiserer avlevering enn innlegging av ny informasjon i databasen i staden for noko anna. Eit anna sentralt spørsmål vil vera om tilsvarande informasjon finst allment tilgjengeleg på anna medium.»

Behovet for avgrensning og nærmere regulering er ikke blitt mindre i dag med den bruken av Verdensveven som i dag er blitt vanlig. På nettet finnes det et stort mangfold. Mye av det som ytres i elektroniske debattfora eller på nettets sosiale møteplasser, har sjangermessig langt mer til felles med muntlige samtaler i private rom og på kafeer, enn den type ytringer som utgis i form av trykt skrift.

Personvernkommisjonen har forståelse for at det er ønskelig med pliktavlevering også av elektronisk materiale. Det finnes en rekke nettpublikasjoner som det er naturlig å likestille med andre publikasjoner, for eksempel *VGnett* eller *Aftenposten.no*. Andre dokumenter, som for eksempel private hjemmesider, er det etter kommisjonens vurdering grunn til å vurdere annerledes. Kommisjonen mener også at det er uheldig at det ikke finnes noen mulighet til å reservere seg, eller å unnta visse typer materiale fra arkivering. Den omstendigheten at mer og mer kommunikasjon foregår digitalt, og at det teknisk sett er forholdsvis enkelt å automatisere innsamling, indeksering og arkivering av digitalt materiale, bør ikke i seg selv innebære at man arkiverer langt mer materiale enn tidligere. Tvert i mot, fordi digitalt materiale er langt mer søkbart og egner seg godt til strategisk informasjonsanalyse og andre former for generell informasjonssøking, bør man være langt mer restriktiv med hvor mye digitalt materiale som samles inn og arkiveres. I og med at det er snakk om permanent lagring, og fordi det er snakk om å lagre innholdsdata i fulltekst, bør det legges klarere føringer på hva slags materiale som skal omfattes av elektronisk pliktavlevering.

13.5 Forslag til tiltak

Dette kapittelet inneholder kommisjonens konkrete forslag til tiltak som bør iverksettes for å styrke personvernet i forhold til mediene.

13.5.1 Medieansvarslov

De nye nettmediene skaper nye utfordringer for personvernet, blant annet fordi mange av rollene som bidrar til produksjon og formidling av innhold i slike media ikke alltid er klart definert. Personvernkommisjonen mener at eventuelle uklarheter er til skade for personvernet. Personvernkommisjonen mener derfor at det bør ryddes opp i både begrepsbruk og regulering på dette området.

Som tidligere nevnt foreslo Ytringsfrihetskommisjonen i 1999 at det ble laget en egen medieansvarslov. Personvernkommisjonen tror at en slik lov vil være et hensiktsmessig redskap for å få gjort den opprydningen vi mener er påkrevd. Kommisjonen foreslår derfor at det utformes en egen medieansvarslov som definerer roller og fastslår ansvar for alle typer media, dvs. både tradisjonelle forhåndsredigerte media, og nye, elektroniske brukerstyrte og brukerutgitte massemedia og publiseringsarenaer (dvs. blogger og personlige hjemmesider).

Blant elementene en slik lov bør inneholde, vil kommisjonen peke på behovet for en klarere definisjon av redaktørrollen og redaktøransvaret for ulike former for nettbaserte media, samt en grenseoppgang i forhold til ansvar hos andre mediaroller, for eksempel tjenesteyter, slik dette er beskrevet i ehandelsloven. Dessuten, hvordan de prinsipale ansvarsforholdene kan og bør reguleres, i media som i sin art er uten redaktør, eksemplifisert ved det vi i avsnitt 13.3.3 har benevnt som «web 2.0», «egenpublisert», og «person-til-person».

Personvernkommisjonen mener at det er mange hensyn, inklusive personvernhensyn, som tilsier at det bør være mulig å ytre seg anonymt eller med skjult identitet, både på trykk og på nett. Imidlertid ser vi at skjult identitet gjør at enkelte, uten å frykte for å måtte stå til ansvar, sprer ærekrenkelser og ondsinnet sladder og på den måten krenker andres personvern. Også andre rettsstridige ytringer, og da særlig opphavsrettsbrudd, ha-

tefulle ytringer, trusler, spredning av ulovlig pornografi og oppfordringer til lovbrudd og selvmord, gjøres under skjult identitet. Av den grunn mener Personvernkommisjonen at det er viktig at det i media som tillater eller muliggjør ytringer med skjult identitet, finnes et annet klart definert ansvarssubjekt. I den utstrekning tjenestetilbydere, nettverter, tilbydere av fildelingstjenester, og andre, legger til rette for anonyme ytringer, bør disse også ha ansvaret for å forhindre at slike ytringer gjør skade. Som et minimum bør de ha i beredskap et apparat som er tilgjengelig for å motta klager på skadelige ytringer og uten ugrunnet opphold fjerne ytringer som krenker personvernet eller andre lover.

Følgende fem punkter er Personvernkommisjonens forslag til hvilke prinsipper som bør legges til grunn for en medieansvarslov.

1. Ethvert medium kan ha en ansvarlig redaktør, men ut over det som allerede er bestemt i Lov om redaksjonell fridom i media, er det ingen plikt til å ha ansvarlig redaktør. For et medium uten ansvarlig redaktør må det imidlertid defineres et annet prinsipalt ansvarssubjekt.
2. Et medium som har ansvarlig redaktør, omfattes av det særlige redaktøransvaret. Redaktøren kan ikke frita deler av mediet fra dette ansvaret.
3. Kildevernet (anonymitet for opprinnelig ytrer) lovfestes. Kildevernet gjøres imidlertid betinget av at det finnes en ansvarlig redaktør. Et medium uten ansvarlig redaktør kan ikke ha et lovbeskyttet kildevern.
4. For et medium som ikke har en ansvarlig redaktør gjøres det gjeldende at det primære ansvarssubjekt har ansvar for ulovlige ytringer som formidles gjennom mediet. Det innrømmes imidlertid ansvarsfrihet dersom ansvarssubjektet uten ugrunnet opphold sperrer tilgangen til en ulovlig ytring så snart vedkommende får kjennskap til forholdet.
5. Hvorvidt et medium har en ansvarlig redaktør må angis eksplisitt. Både for ansvarlig redaktør og for annet prinsipalt ansvarssubjekt bør det være lett å finne ut hvem vedkommende er og hvordan vedkommende kan kontaktes. En mulig løsning kan være at alle massemedia har plikt til å registrere seg i et eget register (for eksempel lagt til Brønnøysund, Statens Medietilsyn, Redaktørforeningen eller Presseforbundet) med navn og kontaktinformasjon til ansvarlig redaktør eller annet prinsipalt ansvarssubjekt.

13.5.2 Fotografering, og retten til eget bilde

Et av de reguleringsforslagene fra den svenske Integritetsskyddskommittéen[7] som vakte mest oppsikt (og mest strid), var følgende:

> ”I brottsbalken införs en bestämmelse om olovlig fotografering som i princip gör det förbjudet att utan lov fotografera eller filma personer som befinner sig på platser dit allmänheten inte har insyn. Kommitténs förslag innebär att det blir straffbart och förenat med skadeståndskyldighet att utan samtycke fotografera eller filma personer som befinner sig: inomhus i den egna bostaden, hotellrum, klassrom, på sjukhus där personen befinner sig för vård, i omklädningsrum, på toaletter i provhytter, m.m.”

Forslaget var primært rettet inn mot bruk av «skjult kamera» for å filme andre mennesker avkledd i omkledningsrom og lignende, men ble møtt med sterk kritikk fra blant annet pressen, som betraktet den som en anti-paparazzi-bestemmelse.

Også Frankrike har nylig skjerpet lovgivingen på dette området ved å gjøre det straffbart for personer som ikke har nyhetsformidling som yrke å fotografere eller filme voldshandlinger. Denne bestemmelsen er påstått rettet inn mot et ungdomsfenomen kjent som «happy slapping». Dette dreier seg om at en ungdomsgjeng velger seg et tilfeldig offer som bankes opp, at dette filmes med mobilkamera, og at videoen legges ut på Internett for å mobbe voldsofferet.

Som en del av sitt redaksjonelle tilbud har mediebedrifter lagt ut løpende videostrømmer på nettet som i sanntid viser offentlige plasser og veier. Den mest kjente av disse tjenestene er Google Street View, og i USA er tjenesten detaljert nok til at enkeltindivider kan identifiseres. I USA har denne tjenesten helt klart krenket integriteten til noen av de personer som er avbildet, ved at de er vist i krenkende situasjoner (urinering, blotting, beruselse).

Personvernkommisjonen ser imidlertid ikke noe behov for å innføre strengere bestemmelser på foto-området enn de som allerede eksisterer. Bestemmelsen i åndsverksloven § 45c om retten til eget bilde, innebærer at det i de fleste situasjoner vil være nødvendig med samtykke fra den avbildede før et bilde som viser en person gjengis eller vi-

[7] Integritetsskyddskommittéen (Sluttbetänkande SOU 2008:3) ble satt ned av den svenske regjeringen i 2004 for blant annet å utrede «lagstifting som rör den personliga integriteten».

ses offentlig. Når det gjelder publisering av billedopptak gjort ved fjernsynsovervåkning og løpende videostrømmer, er disse regulert av personopplysningsloven §§ 36-41. I praksis innebærer dette at slike videostrømmer bare vil kunne vises offentlig dersom de ikke formidler personopplysninger, dvs. at opplysninger som kan knyttes til en personlig identitet som ansikter og bilskilter må sladdes eller på annen måte skjules/anonymiseres.

Når det gjelder bruk av «skjult kamera» i avkledningsrom og lignende rammes dette allerede av flere bestemmelser i straffeloven, i første rekke § 390a som forbyr «skremmende eller plagsom opptreden eller annen hensynsløs adferd». For kommisjonen virker det uhensiktsmessig å innføre et vidtfavnende fotoforbud for å komme slik adferd til livs.

Når det gjelder det franske forbudet mot å fotografere voldshandlinger, vil voldshandlingen i Norge være ulovlig. En eventuell video vil både tjene som bevis mot voldsutøverne, og dersom det kan påvises forbindelser mellom voldesutøverne og de som filmer, kan de siste under gitte forutsetninger tiltales for medvirkning. Videre vil det å legge en slik video ut på nettet utvilsomt være et inngrep i retten til eget bilde (åndsverkloven § 45c) og en krenkelse av privatlivets fred (straffeloven § 390).

Som bl.a. Rodney King-saken i USA viste, kan det at privatpersoner filmer vold avsløre maktovergrep.

Personvernkommisjonen har imidlertid merket seg at Høyesterett i bryllupsfoto-saken kom til at retten til eget bilde ikke ble krenket.

Av den grunn mener Personvernkommisjonen at man i samband med den kommende revisjonen av åndsverkloven bør vurdere bestemmelsen om retten til eget bilde og nærmere presisere hvordan avveiningen gjennom vern av eget bilde (åndsverkloven § 45c) skal være å forstå i forhold til de øvrige lovbestemmelsene og avveiningen mellom EMK artikkel 8 og 10.

13.5.3 Utvidelse av fri rettshjelpordningen

Personvernkommisjonen mener det er uheldig at bare et fåtall saker der det er konflikt mellom mediene og publikum om personvernkrenkelser blir prøvet for domstolene. Vi mener et hensiktsmessig tiltak for å avhjelpe dette er å la fri rettshjelpsordningen utvides til å omfatte visse saker mot mediene, slik at det ikke skal være økonomien som avgrenser den krenkedes mulighet til behandling for domstolene.

13.5.4 Organ for nettytringer

Personvernkommisjonen mener det bør opprettes et eget organ (jf. den nå nedlagte Nettnemnda), som til dels kan bidra til å utvikle gode etiske retningslinjer for nettytringer og dels kan respondere på og løse ulike konflikter i samband med nettytringer.

Som vedlegg 2 til denne rapporten finnes notatet *Nemnd for Internett*. Dette er resultatet av en utredning vedrørende organisering og finansiering av et organ for nettytringer. Utredningen er gjort av advokat Andreas Galtung på oppdrag fra Personvernkommisjonen.

Personvernkommisjonen erfarer at de publiseringsflater som nettet tilbyr dessverre også har resultert i ytringer i form av mobbing, sjikane og ulovlig spredning av personopplysninger, hatefulle ytringer, immaterialrettslige krenkelser (brudd på åndsverklovens regler om opphavsmannens enerett) og publisering av skadelig og harmfullt materiale (jf. Galtung). Ofte er ingen villig til å ta ansvar for slike nettytringer, og det kan være uklart hvem som er rette ansvarssubjekt. Ofte vet heller ikke den som har blitt krenket hvem som står bak ytringen, eller hvor man skal rette en klage.

I mange av konfliktene omkring personvernkrenkende nettytringer har ikke Datatilsynet kompetanse til å behandle saken fordi ytringen faller inn under begrensningen i personopplysningslovens § 7 og derfor utenfor loven virkeområde og tilsynets myndighetsområde. Dersom ytringen fremsettes i et medium som ikke er tilknyttet Norsk Presseforbund og som ikke driver med tradisjonell journalistikk, er det neppe naturlig for PFU å behandle konflikten.

Den tradisjonelle arenaen for slike konflikter er rettsapparatet. Men mange av konfliktene omkring nettytringer, og da kanskje særlig slike som involverer barn og unge (både som krenket og/eller krenker) passer dårlig i rettsapparatet fordi prosessen i rettsapparatet er langsom. I personvernkrenkelser bør det handles raskt for å begrense skadeomfanget. I mange tilfeller vil ikke den krenkede ha midler til å føre rettssak, og den som krenker vil ikke ha midler til å betale eventuell idømt erstatning eller saksomkostninger ved tap. Det er derfor forbundet med en stor byrde, og en viss risiko, å ta en slik konflikt til rettsapparatet.

I notatet konkluderer Galtung med at et klageorgan for nettytringer bør være:

– offentligrettslig basert

- statlig finansiert
- hjemlet i ehandelsloven
- lagt administrativt til Nærings- og handelsdepartementet, alternativt Post- og teletilsynet
- ha mellom fem og åtte medlemmer
- ha retting, sletting og stengning som sanksjon

Personvernkommisjonen mener Galtungs utredning er et godt utgangspunkt for det videre arbeidet med å trekke opp rammene for en hensiktsmessig organisering og finansiering av et slikt organ, med to forbehold:

- Selv om organet organiseres offentligrettslig, mener Personvernkommisjonen at organet bør plasser slik at det blir faglig uavhengig av Kongen og departementet.
- Videre mener Personvernkommisjonen at organet kun skal ha en rådgivende funksjon, og vil således ikke anbefale direkte sanksjonsmuligheter.

Man må regne med at et slikt organ vil bli stilt overfor vanskelige grensedragninger i forholdet mellom personvern og ytringsfrihet, samtidig som dets nytte vil avhenge av at det kan behandle saker raskt, slikt at (antatt) rettsstridige ytringer blir fort fjernet fra nettet. Personvernkommisjonen ser imidlertid at raske avgjørelser ikke alltid er forenlig med korrekte avgjørelser. Det tilsier etter kommisjonens mening at organet kun skal ha en rådgivende funksjon. Da kan forhåpentligvis de fleste sakene løses direkte ved at partene aksepterer organets uttalelse og retter seg etter den – mens de prinsipielle sakene overlates til domstolene å ta stilling til etter en grundigere behandling.

Et organ for Internettkrenkelser må være et frivillig supplement til domstolsbehandling med utgangspunkt i at begge partene ønsker behandling av saken for organet. Dersom en av partene ønsker at konflikten i stedet skal behandles av en domstol, skal ikke organet prøve saken. Organet skal heller ikke erstatte forvaltningsorganer som Datatilsynet eller selvreguleringsorganer som PFU. Dersom disse organene er kompetente til å behandle konflikten, skal den henvises dit. Det bør vurderes om organet skal gis kompetanse til å innvilge fri rettshjelp i saker hvor én av partene velger ikke å følge organets rådgivende uttalelse.

Personvernkommisjonen tenker seg altså organet for nettytringer som et hurtigarbeidende lavterskel-tilbud som kan motta og behandle klager på nettytringer fortløpende, og der de som behandler sakene besitter både redaksjonell og juridisk kompetanse.

Personvernkommisjonen har ikke hatt tid til å lage et detaljert forslag til organiseringen av et slikt organ. Når det gjelder materielle og prosessuelle regler for organets virksomhet, vises det til Galtungs notat.

Når det gjelder rettslig grunnlag for organets virksomhet, viser vi til Galtungs forslag om forankring i ehandelsloven. Som vi tidligere har beskrevet på i avsnitt 13.2.1.1, åpnes det i forarbeidene til ehandelsloven opp for at et «kompetent organ» kan vurdere lovligheten av en nettytring og på det viset avgrense tjenesteyters ansvar. Et slikt organ vil da bare ha en rådgivende funksjon i forhold til tjenesteyter. I og med at de fleste tjenesteytere ikke har noen egeninteresse i å formidle eller sperre for bestemte ytringer, er det imidlertid rimelig å anta at tjenesteytere vil lytte til, og handle etter, de råd et slikt organ gir.

Organet skal kunne fylle to noe ulike funksjoner.

1. Dersom det fremsettes påstand om en nettytring er rettstridig, skal organet kunne vurdere dette. En slik vurdering vil være basert på organets beste skjønn. Dersom organet kommer til at ytringen er rettstridig, vil tjenesteyter ikke lenger være skjermet av ehandelslovens ansvarsavskjæringsbestemmelser dersom tjenesteyter ikke uten ugrunnet opphold gjør ytringen utilgjengelig. Kommer organet til at ytringen ikke er rettstridig, vil tjenesteyter være skjermet fra ansvar for ytringen inntil en domstol ev. kommer til en annen konklusjon. Organets råd vil imidlertid ikke innvirke på ytrerens eller redaktørens eventuelle ansvar.
2. Organet skal kunne bidra til å utvikle gode etiske retningslinjer for nettytringer. Dette innebærer at organet skal kunne utvikle og vedlikeholde et sett med «regler for god nettskikk» etter mønster fra PFUs Vær Varsom-plakat. Organet skal kunne beslutte om en påklaget nettytring er brudd på god nettskikk eller ikke. En uttalelse om hvorvidt en nettytring er brudd på god nettskikk, meddeles partene og offentliggjøres på organets nettsted.

I sitt innspillsbrev til Personvernkommisjonen har Kultur- og kirkedepartementet bedt om at det blir sett «nærmere på problemstillingen rundt rettighetshavernes behov for å forfølge opphavsrettkrenkelser på nettet og hensynet til personvernet».

Når det gjelder organets virkeområde skriver Galtung (ibid.) følgende:

> «Undertegnede er av den oppfatning at en nemnd bør ha et bredt virkeområde og i utgangspunktet kunne dekke de fleste typer av krenkelser på Internett. Om andre ordninger er relevante, kan nemnda ha som oppgave å sende saker som hører hjemme i andre organer [og] institusjoner videre.»

Personvernkommisjonen slutter seg til dette. Et slikt organ bør få mandat til å behandle andre typer nettkrenkelser enn rene personvernkrenkelser, og da særlig immaterialrettslige krenkelser. Etter kommisjonens oppfatning vil behandling i et slikt organ ta bedre vare på personvernrettighetene og rettssikkerheten til den påklagede enn en del av de alternativene som har vært drøftet, nemlig at det utleveres personopplysninger som identifiserer den påklagede til rettighetshaverne eller at tjenesteleverandørene pålegges å overvåke og sanksjonere mot de som benytter tjenesten rettstridig.

Forbrukerrådet, i samarbeid med IKT-Norge, har for øvrig også foreslått at en nemnd bør løse konflikter knyttet til påstander om rettstridig tilgjengeliggjøring av åndsverk på nett (NTB 2008), slik at det vil være naturlig i det videre arbeidet å se på om Forbrukerrådets og IKT-Norges forslag lar seg forene med Personvernkommisjonens forslag.

13.5.4.1 Regler for god nettskikk

«Regler for god nettskikk» er ment som begynnelsen på en normgivende «plakat» som skal angi gode etiske og tekniske retningslinjert for tilbydere av informasjonssamfunnstjenester med hensyn til behandling av personopplysninger og formidling av materiale som kan gripe inn i personvernet og andre problematiske områder. Den er tenkt som et supplement til Vær Varsom-plakaten på områder som er spesifikke for mediale nettjenester og publisering av ytringer på nett.

Flere andre har tatt til orde for utvikling av slike etiske regler, og vi vil særlig vise til den «Best Practices for Online Service Providers» som Electronic Frontier Foundation i USA har utgitt (EFF 2008):

Nedenfor følger vårt utkast til begynnelsen på en slik plakat.

- Ethvert medium som samler inn og/eller behandler personopplysninger om sine brukere skal ha en publisert personvernerklæring som sikrer transparens når det gjelder behandling av personopplysninger. En slik informasjonsplikt følger av personopplysningsloven, men mange såkalte «nettsamfunn» samler inn og behandler personopplysninger uten å oppfylle denne plikten. Personvernerklæringen skal være et generelt informasjonsunderlag for informert samtykke til innsamling og behandling av personopplysninger, og bør blant annet informere om:
  - hva slags personopplysninger som samles inn;
  - hva innsamlete personopplysninger blir anvendt til;
  - andre forhold som den enkelte vil kunne trenge for å forutse mulige konsekvenser av at personopplysninger om dem blir lagret;
  - hvilke innsynsrettigheter som gjelder for den enkelte;
  - kontaktinformasjon (dvs. hvor og hvordan en bør henvende seg for å få innsyn i informasjon om seg selv);
  - hvilke rutiner som gjelder for sletting, retting og supplering av personopplysninger.
- Ethvert medium skal ha en kontaktadresse der den som mener at deres personvern er krenket av mediet kan henvende seg. Det bør opplyses om hvor lang tid det kan påregnes å gå før henvendelser blir besvart. Henvendelser til kontaktadressen skal besvares uten unødig opphold.
- Feilaktige personopplysninger som publiseres på nett bør korrigeres som følger:
  - Mindre endringer og oppdateringer (feilstavede navn og lignende) kan gjøres fortløpende på den originale nettsiden. At nettsiden er endret, merkes med teksten «Sist endret: [dato]» eller lignende.
  - Mer betydelige rettelser og beklagelser skal fremgå av en tydelig ramme på nettsiden, ev. med lenke til en ny nettside som innholder en beklagelse og/eller korreksjon.
  - En nettside som er funnet å være i strid med god skikk i et kompetent organ skal også merkes med egen ramme og logo, samt med hyperlenke direkte til uttalelsen.
  - En publisert nettside som det ikke lenger er ønskelig spres fordi den utgjør en rettsstridig personvernkrenkelse, skal fjernes fra åpent område på nettet. Man skal videre trekke den tilbake slik at den ikke lenger kan finnes gjennom Google-søk (eller andre søkemotorer). Google tilbyr et selvbetjeningsverktøy (*webpage removal request tool*) som fjerner sider som er fjernet fra

åpent område på nettet fra Googles indeks og cache. Responstiden fra man bestiller sletting og til artikkelen er borte fra Google er vanligvis under 48 timer.

– Nettsteder som tilhører virksomheter som behandler sensitive personopplysninger som knyttes direkte til identifiserende informasjon som personnummer eller fullt navn (eks. trygdekontorer) bør utstyres med en generell «immunisering» mot søkeroboter (jf. kapittel 10.1.4). De sidene som skal være søkbare fra eksterne søkemotorer må eksplisitt unntas fra denne immuniseringen. Også brukerskapt innhold bør være immunisert mot søkemotorer, i alle fall inntil den som er ansvarlig for nettstedet har sett gjennom innholdet og verifisert at det ikke inneholder personopplyninger som det vil være utilbørlig å publisere, eller som på annet vis krenker privatlivets fred.

13.5.5 Slettehjelp

Når personvernet krenkes på nettet er det viktig at det krenkende materialet slettes så snart som mulig, slik at skaden kan begrenses.

I samband med sletting vil det oppstå en rekke praktiske problemer. Er materialet publisert av andre enn den som ønsker å slette det, trenger man å identifisere og lokalisere ansvarssubjektet, slik at forholdet kan påklages. Er det en selv som på grunn av manglende dømmekraft eller ved uaktsomhet har publisert det krenkende materialet, er det som regel ikke tilstrekkelig å fjerne det fra egen tjeneste, man må også få det fjernet fra ymse mellomlagringstjenester (der Googles såkalte «hurtigbuffer» er den mest kjente).

Etter det Personvernkommisjonen erfarer, vil den ansvarlige ofte være imøtekommende i forhold til et forespørsel om å fjerne materiale som krenker personvernet. Likevel går det lang tid før materialet ikke lenger er tilgjengelig fordi mangel på «know-how» forsinker prosessen. Bare det å lokalisere den ansvarlige er en utfordring. Relativt få behersker slike verktøy som WHOIS-oppslag for å lokalisere tjenesteyter og juridisk kontakt for en informasjonssamfunnstjeneste. Når sletting skal effektueres, er det enda færre som kjenner til hvordan de benytter verktøy som Googles *webpage removal request tool* for å fjerne kopier som kan bli liggende i opp til to år etter at originalen er fjernet fra nettet.

Vi mener derfor at det som en prøveordning kunne etableres en tjeneste bemannet med en person med teknisk kompetanse som kan bistå de som får sitt personvern på nettet krenket i oppgavene med å identifisere og oppnå kontakt med ansvarssubjekt og med bruk av selvbetjente slettetjenester. Det er imidlertid ikke meningen at en slik tjeneste også skal yte juridisk bistand i samband med sletting, da dette vil kreve en helt annen type kunnskap, og også langt større ressurser.

Datatilsynet (2008d) har laget en nettside med en del informasjon om hvordan man kan gå fram for å slette informasjon på nett. Dette er en begynnelse, men informasjonen på denne siden er bare i liten grad innrettet på å løse tekniske og praktiske problemer knyttet til sletting av informasjon på Internett.

13.5.6 Offentliggjøring av skattelistene

Personvernkommisjonens delte seg i synet på offentliggjøring av skattelistene.

Flertallet av kommisjonen (13 av 15 medlemmer) har avgitt følgende uttalelse (1):

– Det er viktig av hensyn til samfunnsdebatten at skattelistene er tilgjengelig for publikum. For å hindre misbruk bør slik tilgang både for publikum og mediene kun skje på Skatteetatens nettsider, og mulighetene til søk og sammenstilling av opplysninger bør være begrenset.

Kommisjonens medlem Michael Tetzschner har avgitt følgende særuttalelse (2):

– Kommisjonens medlem, Michael Tetzschner, vil fremheve at opplysninger om personlige forhold, herunder en persons inntekt, faller inn under det loven betegner som personopplysninger. Opplysninger om økonomi for året og tidligere år er noe de fleste vil anse som personlige opplysninger. Sammen med andre, lett søkbare og tilgjengelige parallelle nettopplysninger kan utenforstående danne seg et omfattende og detaljert innblikk i en families eller husstands ulike forhold, herunder økonomien
– Dette medlem mener at fordelene for samfunnsdebatten ikke er dokumentert ved en stadig lettere tilgang til sammenkjeding av opplysninger om enkeltpersoner. Derimot har utviklingen vist at tilbudet om disse personopplysningene inngår i det allmenne underholdningstilbud på nettet. De teknologiske søkemotorer gir også nye muligheter for «scanning» av flere kilder ut fra gruppetilhørighet, for å se hvem som ender «i garnet». I forhold til lister der en i utgangspunktet må søke med tanke på en konkret person, er det er lettere å tenke seg at

et konkrete søk er saklig begrunnet enn generell scanning.
- Dette medlem mener at det er et innbygget misbrukspotensial i mengden og tilgjengeligheten av slike opplysninger. Dette representerer en uforholdsmessig ulempe for den enkelte, i forhold til det som oppnås. Hvilken ulempe den enkelte subjektivt føler, vil variere sterkt. Avgjørende vekt vil i et fritt samfunn måtte legges på de som føler innsyn i personlige forhold som ubehagelig, selv om de skulle utgjøre et mindretall.
- Dette medlem vil mene at det er prinsipielt problematisk at informasjon innhentet av myndighetene for andre formål gis videre til allmennheten over hodet på den det gjelder. Dette strider med prinsippet om at det i første rekke den enkelte som i et fritt samfunn har eiendomsretten til opplysninger om seg selv. Dagens praktisering legger altså risikoen for misbruk på enkeltmenneskene, uten forespørsel eller saklig begrunnelse.
- Dette medlem viser til at hensynet til pressens innsyn i offentlige personers forhold ivaretas gjennom pressens rekvisisjon av kredittopplysninger. Behovet for allmennhetens innsyn kan ivaretas ved utlegging av skattelister i vedkommende kommune innen en begrenset periode, for eksempel på tre uker. Forøvrig gir dette medlem sin subsidiære støtte til de tiltak i personvernfremmende retning som kommisjonens medlemmer går inn for under punkt (1) over.

Kommisjonens medlem Gunnar Flikke har avgitt følgende særuttalelse (3):
- Opplysninger om hvor mye den enkelte bidrar med til fellesskapet, bør være lett tilgjengelig for alle interesserte. Åpenhet på dette området har lange tradisjoner i Norge, og er viktige opplysninger i den offentlige samfunnsdebatten. Fakta fra de offentlige skattelistene har vist seg å være helt avgjørende informasjon både når skattenivå og formen på skattlegging er blitt diskutert.
- Det er ikke avdekket «misbruk» av denne typen informasjon som tilsier at den lovmessige tilgangen til data bør strammes inn. Ønsker man en grundig politisk debatt om skattesystemet hvor alle har like muligheter til å delta, er det viktig at disse fakta er lett tilgjengelig for alle og kan brukes til å sammenligne og analysere.
- Å begrense mulighetene til søk og sammenstilling av opplysninger vil dessuten gjøre det vanskelig å drive effektiv kritisk og undersøkende journalistikk på dette området. Blir konsekvensene av en innstramning at det blir slutt med at redaksjonene får utlevert skattelistene på cd-rom, fratas norske journalister et svært viktig arbeidsredskap.

13.5.7 Pliktavlevering av elektronisk materiale

Selv om det finnes lovhjemmel for innsamling av elektroniske dokumenter, mener Personvernkommisjonen at personvernhensyn ikke er godt nok tatt vare på i planen for pliktavlevering av elektronisk materiale som er under utvikling i Nasjonalbiblioteket. I samband med denne planen bør konsekvensene for personvernet utredes, videre hvordan uheldige konsekvenser for personvernet kan reduseres.

Personvernkommisjonen vil særlig peke på tre mulige tiltak:
1. Det bør være mulig å reservere seg fra innsamling og arkivering, enten ved at Nasjonalbiblioteket pålegges å følge Robot Exclusion Protocol, eller på en annen hensiktsmessig måte.
2. Det bør finnes gode og hensiktsmessige mekanismer for å fjerne materiale som er lagt rettsstridig ut på nettet, fra arkivet, ikke bare belegge det med klausul.
3. Det må utarbeide klare retningslinjer for tilgang og bruk av materialet, herunder hvorvidt mottaker har plikt til å anonymisere identifiserbare opplysninger når formålet med bruk av opplysningene er oppfylt.

13.5.8 Internasjonalisering av nettregulering

Siden nettet er internasjonalt, bør Norge være en aktiv pådriver for at regulatoriske tiltak med sikte på å styrke personvernet på nettet spilles inn i relevante internasjonale fora der Norge deltar, med tanke på internasjonalisering og samordning av tiltakene.

Dette gjelder for eksempel tiltenkte mekanismer for konfliktløsning og fjerning av personvernkrenkelser (jf. det tiltenkte organet for nettytringer). Men norske myndigheter bør også ta opp avtalepolitiske spørsmål vedrørende for eksempel det faktum at amerikanske aktører som Amazon, Google og Facebook kan henvende seg til norske

mediebrukere med avtaler som norske media er avskåret fra å bruke.

Dette området går gjerne under uttrykket «internet governance» og omfatter institusjoner og arenaer som Den internasjonale teleunionen (ITU), Internet Corporation for Assigned Names and Numbers (ICANN), Internet Governance Forum (IGF), og World Association of Newspapers (WAN). Fra Norge deltar bl.a. Post- og teletilsynet (PT) og UNINETT Norid AS i en del slike internasjonale fora, og har sannsynligvis også bedre oversikt enn kommisjonen om hvordan internasjonalisering av nettregulering kan gripes an.

Kapittel 14
Personvern for barn og unge

I dette kapittelet behandles spørsmålet om personvern for barn og unge. Denne gruppen omfatter i utgangspunktet personer som er under myndighetsalder, det vil si 18 år. Barn har de samme rettigheter som voksne når det gjelder personvern, men i tillegg er barn gitt et særskilt internasjonalt vern gjennom FNs barnekonvensjon. I artikkel 16 heter det at:

> «Intet barn skal utsettes for vilkårlig eller ulovlig innblanding i hans eller hennes privatliv, familie, hjem eller korrespondanse og heller ikke for ulovlige angrep mot hans eller hennes ære eller omdømme. Barnet har rett til lovens beskyttelse mot slik innblanding eller slike angrep.»

Også i nasjonal rett finnes det særskilt lovgivning som har betydning for barns personvern, for eksempel i barneloven. Barn og unge har rett til gradvis økende innflytelse når det gjelder spørsmål som angår deres eget personvern. Se mer om dette nedenfor.

Begrepet personvern blir gjerne forbundet med individets interesse i å kontrollere formidling og bruk av personopplysninger som angår en selv. Personvern innebærer blant annet å beskytte personers autonomi og integritet. Personvernfremmede tiltak for barn og unge må være utarbeidet med tanke på at barn og unge er i en utviklingsprosess og at de derfor trenger særlig beskyttelse. De er også i en modningsprosess hvor de utvikler identitet og evne til selvbestemmelse. Barn og unge er i tillegg avhengige av støtte fra andre for å kunne ivareta rettighetene sine. De som forvalter barn og unges interesser, for eksempel ved å samtykke på deres vegne, skal handle til barnas beste, ikke for å eksponere seg selv eller fremme egne interesser.

Personvernet skal blant annet beskytte privatlivets fred. Familien er en sosial enhet som befinner seg mellom det offentlige og det private. Foreldre har stor selvråderett med hensyn til hvordan de vil oppdra barna sine, men krenkelse og overgrep innad i familien er ikke tillatt. I noen tilfeller vil det å beskytte barns personvern og integritet innebære at man må gripe inn i områder som ofte betraktes som arenaer for privatliv og selvbestemmelse.

Retten til privatliv og personvern er en forutsetning for individets mulighet til å opprette og vedlikeholde forskjellige sosiale relasjoner til andre personer. Ethvert individ skal ha en viss innflytelse på hva andre vet om ham eller henne, slik at det blir mulig å utvikle sosiale relasjoner upåvirket av informasjon som er gitt til andre personer i andre sammenhenger (Weinreb 2000, s. 35). Barn og unge har ulike roller. De har roller som sønn, datter, elev, medlem i musikkorps og idrettslag. Barn må ha mulighet til å påvirke hvilken informasjon som er relevant for hva, hvem og i hvilken situasjon. Barn og unge skal også ha mange roller og delta på flere arenaer i fremtiden. De skal delta i yrkeslivet, på den politiske arenaen og i frivillige organisasjoner. Personvern skal beskytte personers mulighet til å presentere ulike sider ved seg selv, til å kunne velge mellom forskjellige sosiale relasjoner og roller, og til selv å ta stilling til hvordan man skal forholde seg til ulike og kryssende sosiale forventninger (Schoeman 1992, s. 21).

Moderne informasjonsteknologi og økende registrering av personopplysninger utfordrer personvernet. Det er altså viktig at tiltak som skal beskytte barn og unges personvern utarbeides med tanke på det faktum at barn og unge er i en utviklingsprosess hvor de er i ferd med å utvikle sine fysiske, psykiske og mentale kapasiteter, og derfor trenger særlig beskyttelse. Personopplysninger som legges ut på Internett kan bli liggende lenge og kan påvirke de sosiale relasjonene barnet søker å opprette i lang tid fremover. I tilfeller hvor det er foreldrene eller andre voksne som gjør opplysninger om barnet tilgjengelig for allmennheten, bør de vurdere om dette er bilder barna selv vil at skal være søkbare i overskuelig fremtid. Det er imidlertid minst like viktig at barn og unge selv er klar over dette. Før man publiserer bilder fra helgas fest på nettet, bør man kanskje tenke om dette er noe man vil at en fremtidig arbeidsgiver skal ha tilgang til.

Barn og unge tar raskt i bruk ny teknologi. Denne gruppen er også hovedmålgruppen for sosiale nettverkstjenester på Internett, som for eksempel Facebook, Nettby, Myspace og Blink. Barn og unge, så vel som voksne, deltar i slike nettsamfunn for å «chatte», holde kontakt med venner, dyrke interesser og finne kjærester. I tilegg finnes det dedikerte «datingtjenester», der man legger ut en profil om seg selv og sine interesser. Et annet nettsted som kan nevnes i denne sammenhengen er YouTube, som er et av mange nettsteder hvor man kan legge ut filmklipp av alt fra konsertopptak, politiske diskusjoner til filmer av private ferier, fester osv. Her er det ingen forhåndssensur. På slike nettsamfunn og nettsteder har det blitt vanlig å legge ut bilder og opplysninger om seg selv og andre. Nettet brukes altså i stadig større grad som privat informasjonskanal, noe som utfordrer muligheten til et godt personvern.

Bruk av Internett og IKT- kompetanse er etter hvert blitt uunnværlig når det gjelder innhenting av informasjon til lekser og skolearbeid. Ny teknologi legger grunnlag for nye former for samhandling. Nettet er blitt en sosial arena der en kan omgås andre mennesker, få venner, diskutere og dyrke spesielle interesser. Ett av de mest populære nettsamfunnene i Norge er Facebook. Her presenterer brukerne seg selv ved å legge ut en profil som inneholder personlig informasjon, interesser og bilder. Dette kan også inkludere opplysninger som defineres som sensitive opplysninger (se kapittel 13.3.3 om personvern og media). På Facebook kan man skaffe seg venner, sende private meldinger og meldinger som er tilgjengelig for alle i ditt nettverk. For barn og unge har medlemskap i nettsamfunn som Facebook etter hvert fått en avgjørende betydning når det gjelder å vedlikeholde sosiale relasjoner og være informert om det som skjer. Internett gjør det mulig å dyrke interessene sine sammen med andre på tvers av geografiske og kulturelle grenser. Det er også en arena for fri meningsytring og meningsdannelse og har derfor et betydelig demokratisk potensial. Barn og unge i dag vil sannsynligvis benytte seg av nettet til fri meningsytring i langt større grad enn det som har vært vanlig til nå, og nettbasert kommunikasjon er blitt en viktig del av barn og unges hverdag.

På samme måte som voksne har krav på personvern på arbeidsplassen, har barn og unge krav på privatliv på skolen. Fjernsynsovervåkning, overvåkning av PC-bruk og andre former for inngripende overvåkning på skolen reiser grunnleggende spørsmål om hvilke signaler man gir barn og unge når det gjelder å sette grenser for inngrep i den personlige integritet. Hvis barn vokser opp med at overvåkning er et akseptabelt virkemiddel, uavhengig av om problemet kan avhjelpes på en mindre inngripende måte, mister de perspektiver som vil være viktige for samfunnet når barnet blir voksent og skal spille en borgerrolle i vårt demokrati.

14.1 Sentrale problemstillinger

Personvern for barn og unge er spesielt nevnt i Personvernkommisjonens mandat:

> «Barn og unge er ivrige i bruken av nye elektroniske kommunikasjonsformar, t.d. SMS/MMS, «chatting», «YouTube». Unge er difor oftast i forkant i utviklinga av nye tenester og nye måtar å nytte teknologi på. Ein bør difor óg ha særkild merksemd mot denne gruppa.»

Personvernkommisjonen mener at det må rettes særlig oppmerksomhet mot barn og unges bruk av nye media, både fordi de ofte er i forkant når det gjelder bruk av ny teknologi, og fordi de ofte ikke har tilstrekkelig erfaring og kunnskap til å se konsekvensene av å offentliggjøre informasjon om seg selv og andre.

Barne- og likestillingsdepartementet har i sitt innspill til Personvernkommisjonen pekt på en rekke områder de mener utfordrer barn og unges personvern. Departementet oppfordrer kommisjonen til å fokusere på barn og unges holdninger til å publisere bilder og personopplysninger om seg selv og andre, og tilfeller der foreldre publiserer bilder og opplysninger om barna sine. Andre problemstillinger de peker på angår tilfeller hvor personer som har vært i befatning med barnevernssaker blir uthengt på Internett samt personrelaterte problemstillinger angående innsamling av personopplysninger om barn for kommersielle formål.

Personvernkommisjonen vil rette spesiell oppmerksomhet mot de problemene som kan oppstå når foreldre publiserer sensitive personopplysninger om barna sine på nettet. Først og fremst har vi observert at slik publisering utfordrer reglene om foreldrenes samtykkekompetanse og prinsippet om at foreldreansvaret skal utøves i samsvar med hva som er til barnets beste. Publisering på Internett har også en side mot ytringsfriheten, ettersom opplysninger som brukes i forbindelse med opinionsdannende formål, langt på vei faller utenfor personopplysningslovens virkeområde og Datatilsynets myndighetsområde.

Personvernrelaterte problemstillinger på forbrukerområdet er viktige fordi barn og unge er en sårbar gruppe som trenger ekstra beskyttelse mot kommersielle aktørers registrering og bruk av personopplysninger. Denne problemstillingen reiser også samtykkerelaterte spørsmål.

Personvernkommisjonen mener det er viktig å bevisstgjøre unge brukere om rettigheter og plikter på nettet. Barn og unge har ofte ikke det erfaringsgrunnlaget som skal til for å forutse uheldige konsekvenser av å legge ut detaljerte profiler om seg selv og opplysninger om seg selv og andre.

Når det gjelder området personvern for barn og unge, har Personvernkommisjonen valgt å fokusere på personvernrelaterte problemstillinger som følger i kjølvannet av ny teknologi.

14.2 Det rettslige utgangspunktet

I rapportens del II har Personvernkommisjonen gitt en oversikt over regler som gir et særlig vern ved behandling av personopplysninger og generell beskyttelse av den personlige integritet. Disse reglene gjelder både for barn og voksne, og det henvises til det som er beskrevet tidligere.

Når det gjelder temaet personvern for barn og unge, finnes imidlertid både nasjonale og internasjonale regelverk som gir et særskilt vern for denne gruppen. Dessuten kan de generelle reglene om personvern reise særlig problemstillinger og utfordringer når de skal anvendes på barn og unge. Disse vil være gjenstand for drøftelse i dette kapittelet.

14.2.1 Menneskerettighetene

Norge har tiltrådt flere konvensjoner som har betydning for barns rettstilling generelt og barns personvern spesielt. FNs barnekonvensjon av 20. november 1989 og Den europeiske menneskerettighetskonvensjon av 4. november 1950 er særlig sentrale. Begge gjelder direkte som norsk rett gjennom menneskerettsloven, men skal ved eventuell motstrid med andre norske lovbestemmelser gis forrang, se menneskerettsloven § 3.

14.2.1.1 Den europeiske menneskerettskonvensjon og retten til privatliv

EMK artikkel 8 gjelder alle individer – uavhengig av alder – og gir vern av privatlivet også for barn. Bestemmelsen er nærmere behandlet i rapportens kapittel 6.1.3. Det er imidlertid verdt å merke seg at de rettigheter som EMK skal verne om, ikke bare regulerer forholdet mellom individet og eventuelle inngrep fra staten. Bestemmelsen pålegger den norske stat å gi alle barn effektiv beskyttelse mot privatlivskrenkelser foretatt av privatpersoner, også i tilfeller hvor krenkelsen blir påført av barnets foreldre. Den gir også barn krav på beskyttelse i forhold til innsamling, forvaltning og spredning av personopplysninger.

14.2.1.2 FNs konvensjon om barns rettigheter

Barnekonvensjonen har barns spesielle behov for beskyttelse i fokus. Den ble ratifisert av Norge den 8. januar 1991. I fortalen til konvensjonen fremheves det som et generelt prinsipp at barn, på grunn av sin fysiske og psykiske umodenhet, har behov for spesielle beskyttelsestiltak og særlig omsorg. Konvensjonen anerkjenner barnet som et selvstendig individ med uavhengige rettigheter, også i tilfeller hvor barnets interesser er forskjellig fra hva foreldrene måtte ønske. Barnets fulle menneskeverd og integritet skal respekteres, noe som skal komme til uttrykk gjennom barnets mulighet til selv å påvirke sitt liv og få sine meninger hørt. I en felles uttalelse fra barneombudene i de nordiske land uttrykkes det at konvensjonen er et verktøy til «*systematisk å innføre barneperspektivet i beslutningsprosesser og i virksomheter som berører barn og unge*». (Barneombudet et al 1999, s. 6).

Begrepet «barneperspektiv» forklares blant annet som hvordan verden ser ut fra barnets synsvinkel, hvordan barnet ser, hører, opplever og føler i visse situasjoner.

Konvensjonen overvåkes på internasjonalt plan av Barnekomiteen, men det foreligger ingen individuell klagerett etter Barnekonvensjonen, slik det gjør etter EMK. I Norge er det Barneombudet som har til oppgave å følge med på om norsk forvaltningspraksis og rettspleie er i samsvar med barnekonvensjonen.

Barnekonvensjonen har som utgangspunkt at det først og fremst skal tas hensyn til hva som er barnets beste, se artikkel 3 nr. 1 som sier:

> «Ved alle handlinger som berører barn, enten de foretas av offentlige eller private velferdsorganisasjoner, domstoler, administrative myndigheter eller lovgivende organer, skal barnets beste være et grunnleggende hensyn.»

Dette er en generell bestemmelse som ikke hjemler noen spesielle rettigheter eller plikter. Barnets beste skal imidlertid tas med i vurderinger som berø-

rer barnet. Artikkel 3 vil altså være et sentralt tolkningsprinsipp når barns rettigheter skal utledes av konvensjonen for øvrig (se mer i Smith og Lødrup 2006, s. 31ff). I tillegg vil prinsippet være et viktig hensyn når nasjonal rett skal anvendes overfor barn og unge, på samme måte som den tilsvarende bestemmelsen om «barnets beste» i barneloven.

Barns rett til personvern presiseres i artikkel 16:

1. «Ingen barn skal utsettes for vilkårlig eller ulovlig innblanding i sitt privatliv, sin familie, sitt hjem eller sin korrespondanse, eller for ulovlige angrep mot sin ære eller sitt omdømme.
2. Barnet har rett til lovens beskyttelse mot slik innblanding eller slike angrep. »

Konvensjonen gir beskyttelse mot inngrep i privatliv og familieliv i vid forstand. På samme måte som for den tilsvarende bestemmelsen i EMK artikkel 8, vil beskyttelse av barns personopplysninger måtte anses omfattet av begrepet «privatliv». Se mer om personopplysningsvernet etter EMK artikkel 8 i rapportens 16.1.3. Barnekonvensjonens kapittel 16 vil være et relevant utgangspunkt for flere av de drøftelsene som gjøres senere i denne rapporten og som gjelder barns personvern eller bruk av barns personopplysninger.

I artikkel 12 slås det fast at barnet har rett til å uttale seg og at barnets synspunkter skal tillegges behørig vekt:

1. «Partene skal garantere et barn som er i stand til å danne seg egne synspunkter, retten til fritt å gi uttrykk for disse synspunkter i alle forhold som vedrører barnet, og tillegge barnets synspunkter behørig vekt i samsvar med dets alder og modenhet.
2. For dette formål skal barnet særlig gis anledning til å bli hørt i enhver rettslig og administrativ saksbehandling som angår barnet, enten direkte eller gjennom en representant eller et egnet organ, på en måte som er i samsvar med saksbehandlingsreglene i nasjonal rett.»

Bestemmelsen innebærer at man skal ha respekt for barnets egne meninger og at barnets mening skal høres og tillegges vekt i beslutninger som vedrører dennes situasjon og omgivelser.

Barns uttalelsesrett og medbestemmelsesrett etter barnekonvensjonen vil være et viktig utgangspunkt når man skal vurdere barnets rett til å bli hørt i saker som gjelder deres privatliv og bruk av personopplysninger, herunder vurderinger knyttet til samtykkekompetanse. Nødvendige innskrenkninger i barns rett til selvbestemmelse må ta utgangspunkt i hva som er barnets beste.

I forlengelsen av dette slås det fast i artikkel 13 at barn har krav på ytringsfrihet. Bestemmelsens første ledd lyder:

> «Barnet skal ha rett til ytringsfrihet; denne rett skal omfatte frihet til å søke, motta og meddele opplysninger og ideer av ethvert slag uten hensyn til grenser, enten det skjer muntlig, skriftlig eller på trykk, i kunstnerisk form eller gjennom en hvilken som helst uttrykksmåte barnet måtte velge.»

Denne bestemmelsen mener kommisjonen er et sentralt utgangspunkt når det gjelder barns rett til å kommunisere elektronisk, samt benytte for eksempel Internett til informasjonsinnhenting eller som en arena for å ytre sin mening.

14.2.2 Personopplysningslovens samtykkebestemmelser

Personopplysningslovens regler vil i utgangspunktet gjelde for behandling av personopplysninger om barn og unge innenfor alle samfunnsområder og sektorer.

Spesielt for denne gruppen er at de er mindreårige, noe som reiser flere problemstillinger i forhold til spørsmål om samtykkekompetanse. Skal det innhentes samtykke fra barnet selv, av foreldrene eller fra begge? Hva kan foreldrene gi samtykke til på vegne av barnet, og hvilke skranker finnes det for foreldrenes adgang til å bruke personopplysninger om egne barn? Når har foreldrene rett til innsyn i opplysninger om barnet? Et annet aspekt er håndhevelse av loven når opplysningene behandles (brukes) av barnet selv, for eksempel når barn/unge publiserer bilder av andre på Internett.

Det følger av de alminnelige reglene i personopplysningsloven §§ 8 og 9 at innhenting og bruk av barn og unges personopplysninger som hovedregel skal baseres på et samtykke, enten fra barnet selv eller fra dennes foresatte. I forarbeidene til loven er det uttalt at «for mindreårige […] som ikke kan samtykke selv, må spørsmålet om samtykke skal gis vurderes av vergen» (Ot.prp. nr 92 (1998-99), s. 103). I Datatilsynets praksis er det lagt til grunn at når barnet når en viss alder, vil det selv ha både samtykkekompetanse og eventuell nektelseskompetanse.

Hvem som kan avgi et gyldig samtykke, barnet og/eller foreldrene vil måtte vurderes konkret i lys av alder, modenhet og hva slags opplysninger

det er snakk om. Barnelovens generelle regel om gradvis selvbestemmelse vil være relevant her, se nedenfor. Det viktigste er at barnet må være i stand til å se rekkevidden og konsekvensen av å gi fra seg sine personopplysninger, hvis ikke vil samtykket ikke anses tilstrekkelig informert.

Datatilsynet og Forbrukerombudet har utarbeidet en veiledning om barn og unges samtykkekompetanse (Datatilsynet 2004). Veiledningen er basert på prinsippet i blant annet barneloven om barns rett til gradvis selvbestemmelse og gir utrykk for anbefalte aldersgrenser på ulike områder. I følge veiledningen kan mindreårige som har fylt 15 år som hovedregel selv samtykke til innhenting og bruk av egne personopplysninger. Dette gjelder imidlertid kun for forholdsvis trivielle opplysninger, som rene kontaktopplysninger som skal brukes til formål som er oversiktlige for barnet selv. Eksempler på slike formål er administrasjon av konkurranser og klubber. Den som samler inn opplysningene må uansett foreta en konkret vurdering av om den mindreårige forstår hva vedkommende er med på og ta særlig hensyn til opplysningenes art og omfang. Det må også iverksettes tiltak for kontroll av barnets alder.

Innhenting av sensitive personopplysninger bør i følge veiledningen normalt forutsette foreldrenes samtykke. Det fremheves videre at bilder med erotisk eller seksualiserende innhold skal behandles som sensitive personopplysninger. Det uttales også at det ikke kan samles inn personopplysninger om andre personer fra mindreårige.

Etter Personvernkommisjonens oppfatning vil slike retningslinjer være viktige når man skal vurdere barn og unges kommunikasjon via Internett samt publisering av bilder etc., se nedenfor.

Personopplysningslovens og barnelovens generelle regler vil suppleres av bestemmelser i spesiallovgivningen, og her kan det finnes særskilte regler om når umyndige har samtykkekompetanse. Eksempelvis følger det av pasientrettighetsloven § 4-4 at mindreårige som hovedregel selv kan samtykke til helsehjelp når de har fylt 16 år. I helseregisterloven § 5 er det slått fast at barn helt ned til 12 år kan ha samtykkekompetanse ved behandling av helseopplysninger, når det av grunner som bør respekteres ikke er ønskelig for den mindreårige at opplysningene gjøres kjent for foreldrene eller andre med foreldreansvar. Etter adopsjonsloven skal barn over 12 år samtykke til adopsjon, og barnet skal fra fylte 7 år gis anledning til å uttale seg. Retten til å bli hørt gjelder også for yngre barn som ut fra alder og modenhet vurderes å være i stand til å danne seg egne synspunkter.

Spørsmålet om samtykke er særlig problematisk i forbindelse med barn og unges internettbruk. Dette gjelder både i forhold til om barnet er i stand til å se omfanget av og konsekvenser av publisering av for eksempel bilder og tekst, og i forhold til vurderingen av om barnet er gammelt nok til å ta beslutningen om publisering.

Etter det Personvernkommisjonen har erfart reiser saker hvor foreldre publiserer opplysninger om og bilder av egne barn på Internett særlige utfordringer i forhold til spørsmålet om samtykkekompetanse. Personvernkommisjonen har redegjort nærmere for denne problemstilingen i kapittel 14.3.5.

I kapittel 14.3.6 nedenfor vil Personvernkommisjonen også peke på noen utfordringer som oppstår når det gjelder samtykke fra barn til bruk av personopplysninger for markedsføringsformål.

14.2.3 Barnelovens regler om foreldreansvaret og barnets beste

Også barneloven har regler som får betydning for barns personvern, både når det gjelder håndteringen av deres personopplysninger og ivaretakelsen av barnets personlige integritet.

Et viktig utgangspunkt er de pliktene foreldrene har overfor egne barn, både når det gjelder å utøve omsorg for barnet og retten til å bestemme for barnet i personlige forhold. Dette er nærmere regulert i barneloven § 30 flg. Foreldrene har rett og plikt til å bestemme for barna når de ikke selv har forutsetninger for å treffe fornuftige og begrunnede avgjørelser. Foreldreansvaret skal utøves ut fra barnets interesser og behov. Slike «personlige forhold» må også gjelde tilgang til og bruk av informasjon som beskriver barnet og iverksettelse av tiltak som kan krenke barnets psykiske og fysiske integritet.

Etter hvert som barnet vokser til, har det både medbestemmelses- og selvbestemmelsesrett, avhengig av alder og grad av modenhet, se §§ 31 og 33. Det foreligger en plikt til å høre barnets mening fra fylte 7 år, og fra fylte 12 år skal barnets mening tillegges stor vekt. Reglene om selvbestemmelse i barneloven § 33 er av betydning når man skal tolke samtykkekravene i andre lover.

Et sentralt fokus i norsk barnerett er hva som er til barnets beste. Dette får betydning for tolkningen av andre regler som regulerer forholdet mellom foreldre og barn, fordi foreldreansvaret skal utøves til barnets beste. I Personvernkommisjonens arbeid har det vært tydelig at prinsippet om barnets beste blir stilt overfor nye utfordringer når

det gjelder foreldrenes publisering av opplysninger og bilder av egne barn på Internett. Se særlig avsnitt 14.3.5 nedenfor.

14.2.4 Ivaretakelse av personvernet i opplæringsloven og barnehageloven

I løpet av skolegangen vil det bli samlet inn store mengder informasjon om det enkelte barn. Som eksempler kan nevnes klasselister, meldinger mellom hjem og skole, dokumenter med vurderinger og karakter, resultater fra nasjonale prøver og utvisningsvedtak. Her vil det fremkomme både trivielle opplysninger og langt mer sensitiv informasjon, noe som gjøre at personvernet utfordres i større eller mindre grad.

Det vil også foregå informasjonsflyt mellom skolen og skoleeier. For eksempel er det lovens utgangspunkt at kommunen/fylkeskommunen gjør vedtak om spesialundervisning for den enkelte elev, og kommunen skal ha halvårsrapporter for hver enkelt elev som har spesialundervisning. I skolemiljøsaker, som for eksempel mobbesaker, vil det bli nedtegnet opplysninger om både den som krenker og den krenkede. Personvernet utfordres ellers av den økende bruk av datamaskiner og Internett i opplæringen, både ved bruk av IKT-baserte læringsplattformer og elevenes egen bruk av datamaskin.

Opplæringsloven har ingen direkte bestemmelser om barns personvern eller behandling av personopplysninger og vil i stor grad suppleres av personopplysningsloven, barneloven og annet regelverk som gjelder for barn og unge. Det er imidlertid forutsatt i lovens formålsbestemmelse at alle i skolen «skal arbeide for å hindre at elevar, lærlingar og lærekandidatar kjem til skade eller blir utsette for krenkjande ord eller handlingar», jf. § 1-2.

Opplæringsloven inneholder dessuten flere bestemmelser som forutsetter behandling av personopplysninger, for eksempel § 15-3 som pålegger skolen å gi opplysninger til barneverntjenesten ved mistanke om omsorgssvikt og § 14-1, 4. ledd som pålegger både de som er ansvarlig for opplæring og de som får opplæring å gi opplysninger til bruk for evaluering og rapportering. Lovens § 15-1 om taushetsplikt, med henvisning til forvaltningslovens regler, er relevant for personvernet da den ivaretar hensynet til konfidensialitet.

For førskolebarn vil barnehageloven være relevant. Også her er det regler om utlevering av opplysninger til sosialtjenesten og barneverntjenesten, se §§ 21 og 22, samt en presisering av forvaltningslovens regler om taushetsplikt.

14.3 Kommisjonens observasjoner

14.3.1 Innledning

Personvernkommisjonen gjennomførte et åpent seminar om personvern for barn og unge den 6. mars 2008. Formålet med seminaret var å skape offentlig debatt og refleksjon rundt dette emnet, samt å hente innspill til kommisjonens videre arbeid. På det åpne seminaret deltok representanter fra en rekke organisasjoner/etater, herunder Barneombudet, Landsrådet for Norges barne- og ungdomsorganisasjoner (LNU), Datatilsynet, Utdanningsdirektoratet, Elevorganisasjonen og Medietilsynet. Hovedfokuset lå på barn og unges nettbruk, vaner og holdninger og spørsmålet om hvordan ny teknologi utfordrer barn og unges personvern.

De problemstillingene som ble belyst på seminaret kan deles inn i fire hovedområder:

1. Barn og unges holdninger til å publisere bilder, filmer og opplysninger om seg selv og andre.

   Flere av deltakerne understreket behovet for at barn og unge må bevisstgjøres om regler, rettigheter og plikter som gjelder på nettet. Dette gjelder særlig avveininger mellom ytringsfrihet og personvern.
2. Markedsføring og personvern.

   Det er kjent at mange websider samler informasjon om brukerne til kommersielle formål. Barn og unge gir ofte fra seg personopplysninger via konkurranser, spill og nettsamfunn. Når behandling av personopplysninger er en del av markedsføringsmetoden, gjelder både markedsføringsloven og personopplysningsloven. Ingen av disse lovene har spesielle regler for behandling av barn og unges personopplysninger.
3. Barn og unges rett til privatliv i forhold til skole, offentlige myndigheter og foreldre.

   Datatilsynet har pekt på at både skoler og barnehager i stadig større grad innretter seg i retning av at det skal være mulig å følge barns hverdag på nettet. Selv om disse tiltakene virker relativt uskyldige og er innført for gode formål, så bidrar de til å støtte opp om en utvikling der foreldre i stadig større grad kan bruke teknologiske verktøy for å følge med på barnas bevegelser. Dette bidrar i sin tur til å krympe barnets privat rom. Under dette punktet ble det også reist spørsmål om personvern for de aller

minste barna. Det ble påpekt at de som arbeider i barnehagen ikke alltid har nødvendig kunnskap om juss og etikk i forhold til bruk av teknologiske verktøy, eller når det gjelder hvilke lover som gjelder ved publisering av bilder på Internett og distribusjon av bilder på CD eller minnepinne. Det ble påpekt at spørsmål som angår personvern for barnehagebarn er lite gjenstand for offentlig debatt.

4. Foreldres og barns rettigheter når det gjelder det å publisere bilder, filmer og opplysninger om egne barn.

   I det siste har vi sett flere tilfeller der foreldre publiserer informasjon om barna sine på nettet. Dette gjelder både uskyldige «skrytebilder», og mere alvorlige situasjoner der barn blir vist fram i ekstremt sårbare situasjoner for eksempel i forbindelse med omsorgsovertakelse.

Det er viktig å være oppmerksom på at det er flere områder som er viktig for barn og unges personvern. Dette gjelder for eksempel på helserelaterte områder, noe som omhandles særskilt i kapittel 16, og på medieområdet, se kapittel 13.

Selv om det har vært relativt lite offentlig debatt om barns personvern i Norge, rettes det en del oppmerksomhet mot hvordan teknologi og elektronisk kommunikasjon utfordrer barns og unges personvern. Dette er også noe myndighetene har valgt å satse på. Under regjeringens tiltak 8.8 i Stortingsmelding nr 17 (2006-2007), *Eit informasjonsamfunn for alle*, står det:

> «Det skal settjast i gang tiltak for å sikre at bevvistgjering av barn og unge om personvern og digital dømmekraft står sentralt i undervsninga, gjennom målretta informasjon om teknologiske muligheter og utfordringer på personvernområdet (St.meld. 17, 2006-2007, s. 43) »

Medietilsynets *Trygg bruk*-undersøkelse (Medietilsynet 2008), som er en undersøkelse av barn og unges medievaner, viser at barn og unge har fått større bevissthet om personvern i forhold til nettbruk de siste årene (sammenlignet med 2003). Dette tyder på at opplysningsvirksomhet og holdningsskapende arbeid er viktig, men det er likevel mye som gjenstår. På Personvernkommisjonens åpne seminar om barn og unge ble det påpekt at en av hovedutfordringene når det gjelder denne gruppens personvern er å skape bevissthet om gjeldene regelverk og allmennmoralske normer når det gjelder publisering av bilder og opplysninger om andre.

14.3.2 Tilfredsstillende samarbeid mellom fagmyndigheter?

Det er mange offentlige aktører som jobber med problemstillinger og saker relatert til barn og unge. Innen skolesektoren vil både Kunnskapsdepartementet, Utdanningsdirektoratet, kommunen og fylkeskommunen være premissleverandører, både når det gjelder saker om håndtering og bruk av personopplysninger og spørsmål knyttet til barns personlige integritet. I tillegg har andre offentlige organer kompetanse og myndighet i slike saker, herunder Datatilsynet, Forbrukerombudet, Barneombudet og Medietilsynet.

Det finnes eksempler på samarbeid mellom disse aktørene, blant annet har Datatilsynet og Forbrukerombudet utarbeidet en veiledning for innhenting av samtykke fra barn og unge. Medietilsynet og Datatilsynet har gått sammen og definert tips for trygg bruk av Internett og mobilnett. Også Utdanningsdirektoratet, Teknologirådet og Datatilsynet har samarbeidet, om undervisningsopplegget *Du bestemmer*.

Slikt samarbeid er imidlertid i liten grad formalisert. Det finnes ingen føringer i lovgivningen for hvordan man sikrer samarbeid og samspill i saker som involverer flere parters fagområder. En nærliggende konsekvens av dette er at det vil være forholdsvis tilfeldig, kanskje personavhengig og dessuten styrt av enkeltsaker hvorvidt man oppretter et samarbeid mellom relevante myndigheter. En særlig utfordring vil være å skape samspill mellom statlige ombud/institusjoner og kommunale aktører, som for eksempel grunnskolene.

Dette har også konsekvenser for de som har rettigheter, det vil si barna og deres foreldre. Det er svært vanskelig å vite hvor man skal henvende seg, og hvem som er den rette instansen for konkrete saker, når så mange aktører er involvert.

Personvernkommisjonen mener det er av stor betydning for barn og unges personvern at man sørger for vekselvirkning og samarbeid mellom sentrale aktører på området. Ved å sikre at relevante tiltak og informasjon rettet mot barn og unge når målgruppen, og ved å styrke kompetansen i de respektive fagmyndighetene gjennom samarbeid på feltet, får man en bedre helhetlig beskyttelse.

14.3.3 Holdninger og digital dømmekraft

Personvernkommisjonen mener det er viktig at barn og unge er bevisste på konsekvensene av publisering av egne og andres personopplysninger

på nettet. I rapporten *Fra World of Warcraft til YouTube* av Berit Skog (2008), kommer det fram at Facebook-medlemmer først og fremst bruker Facebook til å se på andres bilder, etterfulgt av å se på andres profiler. Grunnen til at nettopp dette nettsamfunnet er blitt så populært, er at det gir anledning til å følge med på hva venner gjør. Facebook gir dermed brukerne en viss mulighet til «å overvåke» hverandre. Nettstedet overvåker også egne brukere gjennom registrering av adferd og endringer i de ulike profilene. (Dette blir grundigere omtalt i kapittel 13 om personvern og media).

For barn og unge er det å publisere bilder og opplysninger om seg selv og andre blitt en naturlig del av måten å kommunisere med hverandre på. Publisering av bilder og personopplysninger kan imidlertid få uforutsette og langsiktige konsekvenser. Det er ikke alltid like lett å forstå hva det innebærer at informasjon om deg og vennene dine blir lagret for lang tid og at denne kan være av interesse for kommersielle aktører og andre uvedkommende (for eksempel kriminelle aktører).

Tall presentert i rapporten *Trygg bruk* (Medietilsynet 2008), viser at bruk av Internett og digital kommunikasjon er en viktig del av barn og unges hverdag. Alle i aldersgruppen 8-18 år bruker PC til aktiviteter som lekser, surfing, e-post eller chatting. Den viser at 98 % av denne aldersgruppen har tilgang til PC hjemme, hvorav 98 % prosent av denne gruppen igjen har Internett. Over halvparten av gruppen som har tilgang til Internett har egen PC. 72 % av barn og unge mellom 8-18 år har minst én egen e-postadresse, og 78 % oppgir at de «chatter». Blant de eldste ungdommene «chatter» alle. 23 % av barn og unge oppgir at de selv har opplevd at det er lagt ut bilder eller opplysninger av dem uten at de har gitt tillatelse til det. Jenter har i noe større grad opplevd dette enn gutter. Blant de eldste i aldersgruppen, 17-18 år, er det hele 41 % som oppgir at de har opplevd dette. En av konklusjonene er at:

> «…en av de viktigste opplysningsoppgavene når det gjelder barn og unge og deres internettbruk er at de må tenke seg om når de legger ut personlig informasjon på Internett. Bilder og opplysninger som er lagt ut for å dele med venner kan plukkes opp i helt andre sammenhenger enn tiltenkt, og dette må man være bevisst på.» (Medietilsynet 2008, s. 4)

Barn og unge har rett til både personvern og ytringsfrihet. Disse rettighetene er som vi har omtalt ovenfor nedfelt både i den europeiske menneskerettskonvensjonen og FNs barnekonvensjon. Ytringsfrihet gir barn og unge rett til å ytre seg gjennom ulike media, skape debatt, utrykke frustrasjon og fremme saklig kritikk mot for eksempel lærere, skole, offentlige autoriteter og foreldre. Å beskytte barn og unges personvern betyr ikke å legge ned forbud mot at de skal ytre seg eller legge ut informasjon om seg selv, men å sørge for at dette skjer innenfor gjeldende regelverk og i henhold til normer for akseptabel opptreden. Det er for eksempel stor forskjell på saklig kritikk og krenkelser.

Nettet er ikke bare arena for sosialisering, nettverksbygging og meningsytring, men også for konfliktskaping, ryktespredning, trusler og mobbing. Barn og unge må bevisstgjøres i forhold til hvor alvorlig det er å legge ut informasjon som kan skade deres eget og andres omdømme og personlige integritet. Hovedregelen er at alle som publiserer bilder og andre personopplysninger på nettet må forholde seg til personopplysningsloven og det øvrige regelverket for personvern. Det er følgelig de voksnes oppgave å gjøre barn og unge oppmerksomme på hvilke regler som gjelder etter norsk lov og hvilke konsekvenser brudd på disse kan medføre, både i forhold til straffeansvar og/eller erstatningsansvar.

Undersøkelser viser at befolkningen i Norge generelt har stor tillit til at myndigheter og bedrifter ivaretar personvernet på en god måte (se Ravlum 2005b). En av grunnene til at folk ser ut til å bekymre seg relativt lite om personvern er at de føler at de ikke har noe å skjule. Teknologi som griper inn i personvernet blir ansett for å være rettet mot andre, for eksempel de kriminelle og ikke dem selv. Overvåkning og registrering av personopplysninger kan derfor oppleves som noe som gir beskyttelse mot kriminalitet og uro. Teknologirådets rapport fra borgermøter i seks europeiske land viser også at nordmenn er relativt lite bekymret for misbruk. På det norske møtet ble det påpekt at man kanskje ville være mer opptatt av retten til personvern hvis man hadde opplevd krig og urett, enn hvis man har levd i et velfungerende demokrati hele livet (Teknologirådet 2007b). Slike holdninger og mangel på offentlig debatt har kanskje bidratt til at barn og unge er relativt ukritiske med hensyn til å spre informasjon om seg selv og andre gjennom digitale media. Mye tyder på at barn og unge heller ikke tenker så mye over hvordan personopplysninger kan misbrukes av uvedkommende.

Teknologirådets rapport *Holdninger til personvern* (Teknologirådet 2004), som er en undersøkelse av folks generelle holdninger til personvern, viser at ungdommer i mindre grad enn voksne er opptatt av hvilke konsekvenser misbruk av per-

sonopplysninger kan ha. Ungdommene i denne undersøkelsen er mellom 17-19 år. Her er noen eksempler på hva som blir sagt:

> «Jeg tenker ikke over det når jeg gir fra meg informasjon om meg sjøl, jeg tenker at det er ingen som gidder å gjøre noe med det, at det er ingen som kommer til å bruke det. Det er mulig at det er dumt tenkt. Gutt, Oslo.
>
> Man tenker jo at det ikke er så mange opplysninger som er så farlig å gi bort: Jeg forstår ikke helt hva som er så farlig med at det er noen som får tak i navnet mitt og adressen min. Jeg forstår ikke hva de kan gjøre med det. Jente, Oslo.» (ibid.)

Deltakerne ble også spurt om de hadde opplevd å bli fotografert og fått bildet publisert via Internett eller MMS i etterkant. Det var bare de unge deltakerne i undersøkelsen som hadde opplevd dette, og det gjaldt først og fremst bilder som var tatt på fest.

Blant ungdommer er det blitt stadig vanligere å legge ut bilder av seksuell karakter på nettet. I Redd Barnas rapport *På nett med barna* (Aas-Hansen 2007) kan vi lese at ungdommene de har snakket med forteller at det er populært å publisere bilder av seg selv på internettsider der man får poeng for utseendet sitt. Ungdommene har delte meninger om slike steder, men i enkelte vennegjenger er det populært. På nettsteder som dette er det vanlig å lage en profil på seg selv som blir gjort tilgjengelig sammen med bildet. Det viser seg at unge ofte ikke tenker på at det som legges ut på nettet blir liggende lenge, og at det ikke er lett å få fjernet bilder av seg selv.

> «Jeg la ut et bilde av meg selv på deiligst for lenge siden. Etterpå så angret jeg og prøvde å få det bort, men det fikk jeg ikke til. Det var utrolig kjipt. Trude, 8. klasse» (Aas-Hansen 2007, s. 16)

Redd Barna har offentlig kritisert og politianmeldt nettsteder de mener gjør barn til seksualobjekter gjennom å vise fram bilder med seksuelle undertoner av unge jenter og gutter hvem som helst kan komme i kontakt med. Ett av disse nettstedene er deiligst.no.

Anmeldelsen av deiligst.no ble henlagt, og nettstedet opererer fremdeles i skrivende stund. Nettstedet fikk også pålegg fra Datatilsynet om å slette profilen til en da 13 år gammel jente etter klage fra moren (sak med Datatilsynets referanse 2004/1406).

Når det gjelder nettsteder som initierer publisering av bilder, er det viktig å se hen til personopplysningslovens og åndsverkslovens krav om samtykke. Bilder av gjenkjennelige personer/personer som direkte eller indirekte kan identifiseres anses som personopplysninger. Som beskrevet under kapittel 14.2.2 ovenfor, har Datatilsynets lagt til grunn at barn over 15 år kun kan samtykke til bruk av personopplysninger som *ikke* er sensitive. Bilder med erotisk eller seksualiserende innhold kan i noen tilfeller anses som opplysninger om seksuelle forhold.

I disse tilfellene blir spørsmålet om samtykkekompetanse sentralt. Som nevnt finnes det ikke konkrete regler i dagens lovverk for når barn kan ta beslutningen om publisering av personopplysninger på Internett og når det må innhentes samtykke fra foresatte. Vurderingen må tas på bakgrunn av hva slags opplysninger det er snakk om og om barnet er i stand til å se rekkevidden av og konsekvensen av slik publisering. Barns selvbestemmelsesrett står sentralt i norsk barnerett, og foreldrenes eller offentlige myndigheters rett til å gripe inn, når de mener det er til barnets beste, må vurderes i lys av dette.

14.3.4 Digital mobbing og personvernkrenkelser på nettet

Internett er som nevnt en arena for vennskap, sosialisering, innhenting av kunnskap og underholdning, men også for mobbing og trakassering. Digital mobbing er et stadig økende problem. Begrepet «digital mobbing» er relativt nytt og refererer til mobbing gjennom Internett og mobiltelefon. Mobbere bruker media og virkemidler som sms, mms, mobilkamera, e-post, blogger og hjemmesider. Digital mobbing kan være aggressive og krenkende handlinger utført via Internett, mobiltelefon eller e-post (se for eksempel *stopcyberbullying.org*). De elektroniske mediene gjør det mulig for mobbere å være anonyme. Dette gjør trolig terskelen for hva man kan tillate seg lavere enn ved kommunikasjon som skjer ansikt til ansikt. Anonymiteten gjør det også vanskeligere å stoppe mobberne fordi man ikke vet hvem de er.

Eksempler på digital mobbing er å publisere negative og krenkende utsagn om andre, føre liste over personer en ikke liker, publisere rykter og usanne påstander om andre og opprette såkalte hatsider mot andre. På nettsamfunn som Facebook og Nettby fins det grupper som er opprettet for å uttrykke sinne, frustrasjon og hat mot enkeltpersoner og grupper. Hvem som helst kan opprette slike grupper. Det kan skape store problemer for andre, men også for den som legger ut

uønsket materiale. Administratorene av aktuelle nettsteder kan fjerne eller utestenge folk som driver med denne formen for aktivitet, men det er enkelt å lage en ny profil og fortsette mobbingen.

Den digitale mobbingen kan være lettere å skjule enn tradisjonell mobbing. Mange barn tenker kanskje at når foreldre eller lærere ikke ser hva som foregår på nettet, så vil det heller ikke få noen konsekvenser, eller at det som skjer på nettet ikke er så alvorlig som det som skjer i andre relasjoner. Mobbing og trakassering på Internett kan imidlertid i noen tilfeller føles mer alvorlig enn tradisjonell mobbing. Den digitale mobbingen er nærmest irreversibel, da det som havner på nettet blir liggende lenge og fører til at den som blir mobbet føler seg krenket i lang tid fremover.

Politiet får stadig flere henvendelser fra foreldre som er fortvilet over at barna deres er blitt krenket på nettet. Fra 2006 til 2007 økte saker om mobbing, trusler og ærekrenkelse med over 17 prosent i konfliktrådene. Tallet er mer enn doblet siden 2002 (Adresseavisen 2008).

Digital mobbing foregår også ved at noen utgir seg for å være andre og legger ut opplysninger som navn, telefonnummer og adresse. Dette kan forårsake betydelig skade for den det går ut over.

En jurist fra KRIPOS som holdt foredrag på ett av kommisjonens interne møter viste til følgende eksempel: På et populært nettsted i Norge har det blitt laget en falsk profil over en 13 år gammel jente hvor det opplyses at hun ønsker sex med voksne menn og fantaserer om å bli voldtatt hjemme. Profilen inneholdt korrekte og utfyllende personopplysninger. Saken ble politianmeldt, og det viste seg at profilen var opprettet av en person i jentas omgangskrets som hevn og resultat av en uenighet.

Det er viktig at barn og unge bevisstgjøres i forhold til at visse handlinger på nettet kan være straffbare og hvilke konsekvenser lovbrudd kan ha for fremtiden deres. Krenkelser, mobbing og id-tyveri kan rammes av flere straffebestemmelser, og personer over 15 år kan straffes.

I denne sammenheng er det også viktig å fremheve at det finnes andre ansvarssubjekter i for personvernkrenkelser/ulovlig ytringer på Internett, for eksempel for redaktører, tjenesteytere og distributører. I forhold til såkalte «nye» medietyper (hjemmesider, blogger etc.) som barn og unge er storforbrukere av, ser Personvernkommisjonen at dagens regulering av ansvar er utilfredsstillende på flere punkter. Dette er særskilt drøftet i kapittel 13 om media og personvern.

14.3.5 Bruk og misbruk av opplysninger om egne barn

Et av forholdene som angår barn og unges personvern som har fått en del oppmerksomhet i mediene de siste årene, er foreldres publisering av bilder og personopplysninger av barn og unge på Internett. I hovedsak dreier det seg om uskyldige «skrytebilder», som feriebilder og bilder fra bursdager og arrangementer. Personvernkommisjonen erkjenner at digitale fotoalbum som deles med familie og venner er svært vanlig, og når formidling til andre skjer innenfor forsvarlige rammer, er personvernet i stor grad ivaretatt. Graden av tilgjengeliggjøring vil imidlertid være et sentralt moment her. Det er forskjell på å gi bestemor tilgang til et album på et lukket forum og å publisere bilder på en hjemmeside som er tilgjengelig for alle Internettbrukere. Det samme vil gjelde for publisering av andre personopplysninger. Det vil også være av betydning hva slags bilder/opplysninger det er snakk om. Det er tilfeller der foreldre har publisert sensitiv informasjon, som for eksempel opplysninger om helseforhold og dokumenter i barnevernsaker.

På Facebook fins det en applikasjon som heter *I have Kids*. Her kan foreldre lage en miniprofil av barnet sitt med bilder og status. Applikasjonen reklamerer med at foreldre kan vise fram barnet sitt til venner, slik at de får følge med i barnets utvikling, for eksempel når det tar sitt første skritt eller får sin første tann. Man kan også følge med på når venners barn har bursdag og utveksle råd og tips om barn med andre foreldre. Informasjonskanaler og diskusjonsfora av denne typen er ikke nødvendigvis en utfordring for personvernet, men her åpnes det for at foreldre også gir fra seg sensitive opplysninger, da opplysninger om barns fysiske og mentale utvikling er helserelaterte opplysninger.

Representanter fra Barneombudet, Barnevakten, Datatilsynet, Redd Barna og Kripos har i ulike sammenhenger advart mot å legge ut bilder av barn på nettet. Redd Barna er bekymret for at bildene kan gjøre barna mer sårbare for uønskede henvendelser og overgrep. Kripos har påpekt at uskyldige feriebilder kan manipuleres og brukes til pornografisk materiale. Det understrekes at voksne må tenke seg om før de tar irreversible valg på vegne av barn. Foreldre må også huske på at barna, i samsvar med prinsipper i barneretten, har medbestemmelsesrett og selvbestemmelsesrett avhengig av alder og modenhet. Dette tilsier at foreldrene i det minste bør la barna få uttale seg om spørsmålet, når alderen tilsier det.

Vi ser også stadig tilfeller der foreldre publiserer svært utleverende materiell om barna sine. Det kan også dreie seg om sensitive personopplysninger som kommer fram i rettsdokumenter, helsejournaler, psykologirapporter og rapporter fra PP-tjenesten (Datatilsynet 2008c, s. 25).

I enkelte tilfeller publiserer foreldre opplysninger om barna sine i kamp mot barnevernet. Det er kjent at videoklipp av vanskelige situasjoner som har oppstått når barnevernet overtar omsorgen for barn ligger ute på nettet, for eksempel på YouTube.com. De fleste av disse klippene er ikke anonymisert, og gir tilgang til sensitiv informasjon om de barna det gjelder. Det kan være ulike motiver som ligger bak, men barns integritet og personvern blir uansett krenket i disse tilfellene. Her er det snakk om å utlevere historien til barn i en vanskelig livssituasjon til offentligheten. Offentliggjøring av informasjon og opplysninger som kan skade barns integritet bryter med rettslige prinsipper og allmennmoralske normer som understreker at barn er fullverdige mennesker som har krav på respekt og beskyttelse.

Bilder og film av gjenkjennbare personer regnes som personopplysninger. Publisering på Internett innebærer en spredning i tid og rom som det er vanskelig å se omfanget av. Det må derfor utvises særlig varsomhet ved innhenting og bruk av barns personopplysninger.

Publisering av personopplysninger, herunder bilder, på Internett, skal som hovedregel bygge på et samtykke fra den opplysningene gjelder. Dette er nærmere drøftet i rapportens kapittel 14.2.2. Samtykkekravet er særlig problematisk når det er barnets foresatte som publiserer opplysningene, da disse i utgangspunktet vil ha kompetanse til å samtykke på vegne av barnet.

I en henvendelse fra Datatilsynet til Barne- og likestillingsdepartementet av 29. november 2007 (Datatilsynets referanse 07/01840) uttaler tilsynet følgende om denne problemstillingen:

> «Så lenge det foreligger et gyldig samtykke fra foreldrene vil behandling av opplysningene (publiseringen) i utgangspunktet være i samsvar med personopplysningsloven. Dette gjør at Datatilsynet i begrenset grad har hjemmel til å pålegge sletting, selv om tilsynet måtte mene at barnets selvstendige rett til integritet og privatliv tilsier det.»

Bakgrunnen for henvendelsen, var et ønske om å få departementets uttalelse i forhold til om annen lovgivning som regulerer forholdet mellom barn og foreldre kan sies å begrense foreldrenes adgang til å publisere svært sensitiv informasjon om barnet sitt på Internett. For dersom foreldrene i kraft av foreldreansvaret ikke har anledning til å ta denne typen beslutninger, vil dette kunne få betydning for samtykkereglene i personopplysningsloven.

Departementet ga følgende svar til Datatilsynet i brev av 6. mars 2008:

> «Etter vår oppfatning er det likevel usikkert om det i lovgivning som barne- og likestillingsdepartementet har ansvar for finnes skranker som kan være til hinder for denne typen publisering.»

Kommisjonen har hatt dialog med andre fagpersoner når det gjelder disse spørsmålene, blant annet professor Lucy Smith, ekspert i barnerett og medlem av FNs barnekomité. Smith ga tydelig uttrykk for at det er klare grenser for hva foreldre kan samtykke til på barnets vegne på områder hvor de har samtykkekompetanse og at FNs barnekonvensjon artikkel 16 setter grenser for foreldrenes adgang til å legge ut private opplysninger om sine barn på Internett. Dette gjelder også bilder.

Personvernkommisjonen mener det er grunn til å utrede dette spørsmålet grundigere, da det er tydelig at man innen fagmiljøet har ulik oppfatning av om dagens lovgivning er egnet til å ivareta barnas rett til integritet og privatliv. Som vi har redegjort for under kapittel 14.2.3, er det et sentralt prinsipp i norsk og internasjonal barnerett at utøvelse av foreldreansvaret skal skje ut i fra hva som må anses som barnets beste. Dette prinsippet mener kommisjonen må kunne tillegges særlig vekt når man vurderer rekkevidden av samtykkereglene i personopplysningsloven. Det at foreldrene har avgitt et samtykke, betyr ikke nødvendigvis at publiseringen er til barnets beste, og spørsmålet blir hvem som skal ha kompetanse til å overprøve utøvelsen av foreldreansvaret i slike tilfeller og når et slikt inngrep kan forsvares. Personvernkommisjonen vil komme tilbake til spørsmålet under forslag til tiltak i kapittel 14.4.

Problemstillingen berøres så vidt av Barnelovutvalget i NOU 2008: 9 (Med barnet i fokus – en gjennomgang av barnelovens regler om foreldreansvar, bosted og samvær), i punkt 7.4:

> «Fra Barneombudet har utvalget mottatt innspill om at foreldrene i enkelte tilfelle bør fratas muligheten til å samtykke på vegne av barnet til å legge ut opplysninger om barnet på internett. Dette kan for eksempel være detaljer fra en opprivende barnefordelingssak. Utvalget ser at slike saker kan reise særlige spørsmål,

og at det i mange tilfeller ikke er til barnets beste at slike opplysninger legges ut på internett. Men eventuelle lovendringer på dette punkt bør i tilfelle finne sted gjennom personvernlovgivningen, for eksempel ved at Datatilsynet gis større adgang til å gripe inn mot nettsider hvor barns interesser blir krenket.»

Det at foreldre publiserer egne barns personopplysninger på Internett har også en side mot unntaket i personopplysningsloven § 7, om at loven ikke gjelder for publisering av personopplysninger som skjer for opinionsdannende formål. Personvernnemnda har behandlet to saker hvor bakgrunnen var at foreldre – i sin kamp mot barnevernet og relatert til omsorgsoverdragelse – la ut svært sensitiv informasjon om sine barn på nett. Disse sakene og selve problemstillingen er nærmere omtalt i kapittel 13.3 om media og personvern. Her var imidlertid spørsmålet hvorvidt barnevernansatte og fosterforeldre kunne kreve sine personopplysninger fjernet, noe som ble avvist under henvisning til at navnene fremkom som ledd i en ytring av opinionsdannende karakter. Nemnda tok ikke stilling til om publisering av opplysninger om barna var ulovlig på annet grunnlag, for eksempel som følge av FNs barnekonvensjon. I og med at nettsidene ble ansett å falle inn under personopplysningsloven § 7, falt de utenfor Datatilsynets kompetanse til å pålegge sletting. Se mer om dette i kapittel 13.2.3 om media og personvern. Personvernkommisjonen foreslår at det oppnevnes et organ for nettytringer som kan løse tvister i grenseland mellom personvern og ytringsfrihet.

14.3.6 Markedsføring rettet mot barn

Mange nettsteder som retter seg mot barn og unge forutsetter at barnet gir fra seg personopplysninger, for eksempel for å delta i en konkurranse eller spille interaktive spill. Opplysningene blir deretter brukt i markedsføringstiltak mot barnet.

Som nevnt i avsnitt 14.2.2 vil slik innsamling og bruk av personopplysninger reguleres av personopplysningsloven, og det må vurderes konkret om barnet har kompetanse til å avgi et gyldig samtykke til at hennes personopplysninger brukes til markedsføringsformål.

Markedsføringsloven har i dag ingen særskilte bestemmelser om markedsføring som er rettet mot barn, og det er ikke et generelt forbud mot å rette reklame mot denne gruppen. I praksis fra Forbrukerombudet og Markedsrådet har imidlertid markedsføringslovens regler blitt tolket strengere når det dreier seg om markedsføring mot barn. Dette med henvisning til markedsføringsloven § 1 første ledd og forbudet mot markedsføring som er urimelig i forhold til forbrukere eller som for øvrig strider mot god markedsføringsskikk.

Barne- og likestillingsdepartementet har nylig lagt fram et forslag til endringer i markedsføringsloven, der det foreslås å ta inn særskilte bestemmelser om markedsføring rettet mot barn (Ot.prp. nr. 55 (2007-2008)). Det fremheves at bakgrunnen for endringene er et ønske om å kodifisere dagens tolkning og praksis knyttet til eksisterende lovverk.

De nye lovbestemmelsene omhandler først og fremst generelle negative former for markedsføring mot barn og unge (for eksempel reklame som spiller på sosial usikkerhet, frykt, angst eller aggressiv reklame som bruker sex, vold e.l.). Selve lovforslaget inneholder ingen konkrete regler som imøtekommer dagens utfordringer relatert til innhenting og misbruk av barns personopplysninger eller markedsføringsteknikker som spiller på dette. Det nevnes i proposisjonen at «det vil også være mulig å lovfeste dagens praksis knyttet til særlig påtrengende reklame mot barn og unge, samt til innhenting og bruk av barns personopplysninger». De personvernmessige forholdene blir imidlertid ikke videre fulgt opp.

Personvernkommisjonen mener man bør vurdere å lovfeste klarere aldersgrenser for barns samtykkekompetanse i forbindelse med markedsføring mot barn, samt vurdere hvilke krav som skal stilles til hvordan barns alder skal kontrolleres.

Et annet problem som Kommisjonen vil fremheve, er at mange nettsteder som innhenter personopplysinger fra barn gjennom særskilte markedsføringsteknikker opererer utenfor norsk jurisdiksjon. Dersom aktørene opererer fra land med begrenset rettslig regulering av barn og unges personvern, skaper dette utfordringer, også når norske barn benytter tjenestene. Internasjonalt samarbeid på lovgivningssiden bør derfor få større fokus fremover.

14.3.7 Personvern i skolesektoren

Skolen er den samfunnsinstitusjonen som møter alle barn og er derfor den viktigste arenaen for opplæring og danning. Opplæringsloven stiller strenge krav til skolens virksomhet med hensyn til at alle skal ha like muligheter til å oppnå læringsmålene sine og settes i stand til å bli aktive og trygge samfunnsborgere. For å kunne tilpasse

opplæringen, herunder også å lage individuelle planer for enkeltelever (jf. opplæringsloven kapittel 5), trengs det forskjellig type kartlegging og dokumentasjon som normalt vil være personopplysninger. Skolen skal også samhandle med en rekke offentlige instanser utenom skolen, bl.a. PPT, barnevern og helsevesen, der personopplysninger i enkeltsaker har et betydelig omfang. I tillegg er en rekke andre institusjoner og organisasjoner i kontakt med skolen og tilbyr sine tjenester og samhandler på mange arenaer der elever er målgruppe og aktive deltakere. Det gjelder idrettsforeninger, kulturinstitusjoner, bedrifter, utdannings- og forskningsinstitusjoner og enkeltpersoner. Gjennom dette får mange tilgang til informasjon om mange elever, inkludert kjennskap til sensitive personopplysninger.

I dag har skolen en mer åpen organisering enn tidligere og klassestrukturen er endret. Dette gjør at flere lærere må forholde seg til flere elever enn tidligere og de får dermed innblikk i flere elevforhold enn elevene de har et spesielt lærer/lederforhold til. I tillegg krever det utstrakte foreldresamarbeidet der foreldre er forventet å stille opp på mange av skolens aktiviteter, et høyt bevisthetsnivå i forhold til hva foreldre kan få tilgang til av opplysninger om andre elever.

Nye digitale læringsformer, omfattende digital datainnsamling og bearbeiding og bruk av disse, stiller utdanningssystemet overfor personvernmessige utfordringer, både med hensyn til hvilke typer opplysninger som gjøres tilgjengelig og hvilke sikkerhetsmessige tiltak som iverksettes. Det har til nå ikke har vært stor oppmerksomhet rundt slike utfordringer, verken på skolenivå eller administrativt nivå.

14.3.7.1 Kameraovervåkning i skolegården

Kameraovervåkning er et stadig mer utbredt virkemiddel for bekjempelse av kriminalitet, og det er langt på vei blitt en metode som aksepteres uten at alternative løsninger blir gjenstand for diskusjon.

Personopplysningsloven har særlige regler om fjernsynsovervåkning i kapittel VII. Slik overvåkning må ha hjemmel i personopplysningsloven § 8, og i praksis innebærer dette at overvåkningen må være nødvendig for å ivareta en berettiget interesse som overstiger den integritetskrenkelsen den som blir overvåket utsettes for. På steder hvor en begrenset krets av personer ferdes, for eksempel på arbeidsplassen, må det i tillegg foreligge et særskilt behov.

Våren 2008 gjennomførte Datatilsynet flere tilsyn mot kommuner hvor temaet var kommunenes bruk av fjernsynsovervåkning, også på skoler. Tilsynet fremhever i en av rapportene etter kontrollen at de ønsket å foreta en nærmere vurdering av overvåkning som griper inn i barn og unges skolegang og fritid (Datatilsynets referanse 09/00414).

Bakgrunnen for at kommuner overvåker skoler oppgis å være kriminalitetsbekjempelse. Mange skoler er utsatt for skadeverk, som tagging, ruteknusing og generelt hærverk. Innbrudd viser seg også å være et problem. Overvåkningen skjer ofte hele døgnet, også i skoletiden.

Datatilsynet mener at overvåkning av skoleelever mens de er på skolen er meget problematisk. Tilsynet finner støtte for sin bekymring i en uttalelse fra den såkalte artikkel 29 gruppen – et organ i EU med spesielt ansvar for å følge med på hvordan personvernregelverket i EU- og EØS-området etterleves (Art 29 WP 2008). Det fremheves at barn og unge fortjener tilsvarende respekt for sitt privatliv på sin «arbeidsplass» som voksne arbeidstakere. Det fremheves også at motforestillingene mot å overvåke barn og unge ikke bør være lavere enn for overvåkning av voksne – tvert i mot. Barn og unge er enda mer sårbare og har mindre forutsetninger for å sette grenser i forhold til hva man bør finne seg i. Skolen har et spesielt ansvar for hvilke signaler man sender ut til unge mennesker i en formende fase av livet. Det pekes også på at det kan få betydning for barn og unges utvikling av tanker om egen frihet og rett til privatliv om de fra en tidlig alder blir gitt et inntrykk av at kameraovervåkning er en normalitet.

Datatilsynet viser særlig bekymring for den overvåkningen som skjer i skoletiden. Det er i skolegården elevene har sine friminutt/pauser, og tilsynet trekker parallellen til de restriksjonene som finnes for å overvåke pauserommet på en arbeidsplass. Selv om mange unge bruker skolegården som en arena også i fritiden, mener Datatilsynet likevel at overvåkning av skoleområdet etter omstendighetene kan aksepteres mellom klokken 1700 og 0700, der det foreligger et saklig behov for slik overvåkning.

Personvernkommisjonen støtter de vurderingene som er gjort av både EU og Datatilsynet i forhold til fjernsynsovervåkning på skolen. Ureglementert oppførsel fra skoleelever bør følges opp av skolens ansvarspersoner. Deres tilstedeværelse vil antagelig virke langt mer preventivt enn et kamera. Uansett er det de voksnes oppgave å lære barn forskjellen på rett og galt. Slik kommi-

sjonen vurderer det, vil det beste virkemiddelet her være å skape dialog når problemet oppstår, ikke i ettertid når man har avdekket ugjerningen ved gjennomgang av et billedopptak.

Personvernkommisjonen ser heller ikke bort fra at slik overvåkning kan sette uheldige begrensninger på barns utfoldelse i hverdagen. Som nevnt i innledningen skal personvernet blant annet beskytte individets mulighet til å utvikle sosiale relasjoner og til å mestre ulike sosiale roller. Overvåkning kan legge begrensninger på barn og unges sosiale læring, der de oppøver evnen til å differensiere mellom ulike roller og situasjoner. Barn bør ha en privatsfære i skolegården, selv om de i prinsippet befinner seg på et offentlig sted, på samme måte som voksne forventer rom for privatliv også på arbeidsplassen. Skolegården er ikke bare et offentlig sted, men også arena for utvikling av nære vennskaps- og kjærlighetsrelasjoner. Dette er relasjoner vi forventer å utvikle i fred, uten innsyn og innblanding av andre.

Uansett er det ikke tvil om at fjernsynsovervåkning på skolen utfordrer vesentlige personverninteresser, som også barn har krav på at blir ivaretatt. Blant annet gjelder dette interessen i å kunne påvirke hvilke opplysninger som samles inn om en – altså retten til medbestemmelse. Selv om fjernsynsovervåkningen drøftes med personer som har vesentlig grad av beslutningsmyndighet i forhold til iverksettelse av tiltak overfor egne barn (foresatte), må det stilles spørsmål ved om ikke barna selv bør kunne påvirke prosessen. I hvert fall må unge som har oppnådd en viss grad av modenhet få anledning til å bli hørt. Og hvis barna ikke ønsker slik overvåkning, er dette et moment som bør tillegges vesentlig vekt. Barns rett til å bli hørt er noe som særlig fremheves i den tidligere nevnte artikkel 29 gruppens retningslinjer.

Videre utfordrer fjernsynsovervåkning i skoletiden prinsippet om minimalitet, altså at man begrenser innsamling av personopplysninger til det som er strengt nødvendig. Hvis kommunen oppgir at formålet med overvåkning av skolens område er å sikre bygninger mot skadeverk, er det ikke opplagt at hele skolegården må overvåkes. Elevene kan gis flere overvåkningsfrie soner samtidig som skolens interesser kan ivaretas.

Det gjelder dessuten å velge tiltaket som er minst mulig inngripende og sørge for at det er forholdsmessighet mellom mål og middel. Dialog mellom lærere og elever samt veiledning i forhold til hva som er akseptabel adferd i skoletiden, er etter Personvernkommisjonens oppfatning å foretrekke fremfor kontrolltiltak.

Interessen i diskresjon og krav om beskyttelse av privatlivets fred er også sentralt for dette temaet. Som nevnt ovenfor, støtter kommisjonen både EU og Datatilsynets vurdering av at barn fortjener respekt for sitt privatliv på sin «arbeidsplass». De bør kunne forvente «private soner» også i skolegården, det vil si områder hvor de kan opptre fritt og uten at voksne holder dem under oppsikt. Selv om opptakene ikke er tenkt brukt til slik overvåkning av elevene, må følelsen av at det er ubehagelig å bli iakttatt, respekteres.

14.3.7.2 Innsyn i barn og unges skolehverdag

Vi ser en utvikling der skolen i stadig større grad registrerer og lagrer informasjon om elevene. Dette gjelder alt fra navn og adresse til karakterer, fravær, årsak til fravær og anmerkninger. Disse registrene blir i økende grad gjort tilgjengelig på nett, og foreldrene tilbys innsyn.

Flere har problematisert innsyn i barns skolehverdag som et problem som utfordrer barn og unges personvern. Kommisjonen vil påpeke at foreldre har plikt til å følge opp barnas skolegang. Innsyn i barns skolehverdag er en forutsetning for å oppfylle denne plikten. Det er imidlertid viktig at opplysningene ikke er tilgjengelige for andre enn dem de angår og at systemene er utviklet slik at de hindrer lekkasje og snoking.

14.3.7.3 Digitale læringsplattformer, elektronisk registrering av resultater, fravær o. l.

Digitale læringsplattformer (learning managment systems), der elevene mottar informasjon, legger ut informasjon om seg selv, deltar i diskusjonsforum, leverer inn besvarelser osv., kan medføre personvernrelaterte problemer. Eksempler på slike læringsplattformer er *Classfronter*, *It's learning* og *Luv'it*. Her dreier det seg om lukkede rom der bare lærere, elever, eventuelt foreldre og administratorer har tilgang.

Elever og studenter legger ut opplysninger som e-postadresse, telefonnummer og adresse. Noe av det som kan være problematisk med slike rom, er at de ofte er dårlig sikret mot at elevene legger ut sensitive opplysninger om seg selv eller medelever. Det er også dårlig innarbeidede rutiner for lagring og sletting, og det kan synes som om skolene og kommunene mangler tilstrekkelig teknisk kompetanse for å ivareta personvernet i slike systemer.

I de digitale læringsrommene kan det også være invitert inn gjester utenfra som lett kan vide-

reformidle informasjon til andre. I prinsippet kan inviterte gjester koble sammen opplysninger og lage profiler som kan selges videre til kommersielle aktører.

I noen av systemene er det bygget inn ulike mekanismer som gjør det mulig å få innsyn i elevenes aktivitet på læringsplattformen. For eksempel inneholder Classfronter kraftige verktøy for registrering av hvordan den enkelte bruker benytter systemet. Dette innebærer at fagansvarlig kan velge å benytte Classfronter til å registrere når/om en elev har vært pålogget systemet, hvor mange ganger en elev har vært pålogget og hva eleven har foretatt seg (ev. ikke foretatt seg) inne i Classfronter. Formålet med å registrere slike data er blant annet at fagansvarlig skal kunne sørge for tettere og mer forpliktende samhandling mellom skolen og elevene, og mellom elevene innbyrdes, slik at kvaliteten på utdanningen blir bedre.

Mulighetene for å følge den enkelte elevs innsats kan bli enklere med et slikt verktøy, men det er også åpenbart at tett oppfølging kan grense opp mot overvåkning. Det finnes få retningslinjer og det er stort sett opp til den enkelte fagansvarlige å sørge for at bruken av systemene tilfredsstiller lovmessige krav. Digitale læringsplattformer gir mange muligheter og verdifulle bidrag til læring og undervisning. Systemene er i stor grad basert på tillit til brukerne. Det er imidlertid viktig at de som drifter disse systemene har tilstrekkelig teknologisk, juridisk og moralsk kompetanse slik at personvernet blir ivaretatt.

14.3.7.4 PC-overvåkning

I tillegg til de overvåkningsfunksjonene som er bygget inn i de digitale læringsplattformene, finnes det på markedet programvare som gjør det mulig å overvåke hva en som benytter en datamaskin foretar seg. Programmene registrerer gjerne hvilke programmer brukeren starter og hvilke nettsider han eller hun besøker.

I 2007 ønsket enkelte politikere i Fylkestinget i Aust-Agder at videregående skoler i regionen tok i bruk slik programvare for å kontrollere at skolens maskiner i skoletiden ble benyttet til undervisning og ikke til andre ting, som for eksempel å surfe på Internett (Sellevold og Sundsdal 2007). Kommersielle aktører benytter overvåkningsmuligheter for skolens ansatte som et salgsargument for sine produkter. Leverandøren Euroline reklamerer for eksempel for sitt produkt *NetSupport School* med at man kan overvåke bruk av tastatur, applikasjoner og meldingstjenester. På sitt nettsted skriver Euroline bl.a. følgende om produktet:

> «NetSupport School utvider muligheten til å kontrollere applikasjonene ved å ta i bruk overvåkning av Messenger. På denne måten unngår en at meldingsapplikasjoner brukes i klasserommet. NetSupport School gir også muligheter til overvåking av spesielle meldingsapplikasjoner i sanntid. Slik vil læreren ha oversikt over innhold og aktivitetsnivå på all <chatting> i sanntid.»

Personvernkommisjonen innser at det kan være et problem at elever benytter maskiner som er dedikert til undervisningsformål til uvedkommende formål. Å innføre denne typen overvåkning kan imidlertid være et inngrep i den enkeltes personlige integritet. For at slik overvåkning skal oppfylle kravene i personopplysningsloven, må det foreligge et rettslig grunnlag (§ 8) i tillegg til at overvåkningen må være saklig begrunnet (§ 11). Man må også se hen til kravene om forholdsmessighet og proporsjonalitet i EMK artikkel 8. Personvernkommisjonen antar at overvåkning av skoleelevers pc-bruk har mange paralleller til overvåkning av ansattes elektroniske kommunikasjon, og at skoleelever bør ha samme vern mot inngripende tiltak på sin «arbeidsplass». Se om overvåkning av elektronisk kommunikasjon på arbeidsplassen under kapittel 15.3.

Kommisjonen mener det er viktig at de som styrer skolen (politikerne og staben) har et bevisst og kritisk forhold til bruk av overvåkningsteknologi ovenfor elevene og at lovligheten av slike tiltak er gjenstand for utredning og diskusjon i forkant av at systemer implementeres.

14.3.7.5 Rustesting i skolen

Det har i senere tid blitt tatt opp til offentlig debatt at flere videregående skoler i Norge benytter seg av urinprøver for å teste rusmisbruk blant elevene sine. I et oppslag i VG den 14. august 2008 oppgir rektor ved Skogmo videregående skole i Skien at man tar urinprøver av mistenkte elever. Det oppgis i artikkelen at dersom en elev nekter å avgi urinprøve, tilkaller skolen politiet. Urinprøven avgis i et eget rom med enveisrute, der helsesøster kan se eleven som avgir urinprøven for å forhindre at det forekommer juks. Adresseavisa tok opp i en artikkel publisert den 12. mars 2007 at over halvparten av de videregående skolene i Sør-Trøndelag ønsker å innføre en ordning med rustesting av elevene gjennom urinprøver.

Kunnskapsministeren ble den 10. april 2008 stilt spørsmål om hjemmelsgrunnlaget for rustesting av elever i videregående skoler (dokument nr. 15:926 for 2007-2008), og i sitt svar 18. april 2008 sier statsråden følgende:

> «Opplæringsloven inneholder ikke bestemmelser som hjemler eller på annen måte regulerer rustesting av skoleelever. Slik testing av elever er heller ikke regulert i annet regelverk. Dette innebærer at skolen ikke kan kreve at elever blir rustestet. Testing av elever må foregå på frivillig basis etter at det foreligger et informert samtykke fra eleven. Et samtykke til rustesting må omfatte alle sider av testopplegget. Dette innebærer at det må være enighet om regelmessigheten av testingen, sanksjoner ved positive tester og det praktiske knyttet til gjennomføringen av testingen, herunder også det ledsagende personalets kjønn. Eleven har derfor naturligvis rett til å velge å ikke delta i rustesting hvis eleven ikke samtykker i hvordan testingen skal gjennomføres. Jeg vil avslutningsvis understreke at et fravær av samtykke til rustesting ikke kan medføre at eleven blir behandlet som om en eventuell mistanke om rusmisbruk er bekreftet eller styrket. Det betyr at det heller ikke kan være forbundet med noen former for sanksjoner å motsette seg testing.»

Personvernkommisjonen mener at tvungne urinprøver er et alvorlig inngrep i elevers privatsfære som krever klar rettslig forankring. Det blir desto mer alvorlig når en skole gjennomfører urinprøven på et slikt vis som Skogmo videregående, der en helsesøster eller andre kan observere at eleven gir fra seg urinprøven.

Adgangen til å gjennomføre rusmiddelkontroll på en arbeidsplass (vaktselskap) har vært gjenstand for vurdering i Personvernnemnda (klagesak 2005/6). I et arbeidsforhold vil iverksettelse av kontrolltiltak måtte følge reglene i arbeidsmiljøloven kapittel 9. Her er det krav om at tiltaket er saklig begrunnet og at det ikke innebærer en uforholdsmessig belastning for arbeidstakeren. Videre behandling av personopplysninger som utledes etter analyse av urinprøver reguleres av personopplysningsloven. I ovennevnte sak kom Personvernnemnda til at samtykke ikke var tilfredsstillende hjemmelsgrunnlag for behandling av personopplysninger etter rusmiddelkontroll på generelt grunnlag, da det kan stilles spørsmål ved om samtykket er avgitt frivillig. De konkluderte også med at rustesting av samtlige ansatte ikke kunne anses som saklig begrunnet i virksomheten.

Personvernkommisjonen mener at skoleelever ikke skal ha noe dårligere vern mot inngripende kontrolltiltak enn det arbeidstakere har, og at samtykke fra elevene er tvilsomt som rettslig grunnlag. Elevene står i et avhengighetsforhold til skolen, og det er vanskelig å tenke seg at noen vil nekte når konsekvensen av dette er at politiet innblandes. Det kan følgelig stilles spørsmål ved om samtykket kan anses frivillig.

Personvernkommisjonen mener at dagens praksis i enkelte videregående skoler må opphøre inntil rettstilstanden på området er avklart. Personvernkommisjonen vil uansett anbefale at myndighetene utviser stor forsiktighet med å lovhjemle en eventuell adgang til å foreta rustesting i skolen, da det kan stilles spørsmål ved om et slikt inngrep er forholdsmessig og nødvendig sett hen til kravene i EMK. Det må vurderes om ikke rusmisbruk blant skoleelever kan avdekkes og avhjelpes gjennom mindre inngripende metoder.

14.3.7.6 Personregistre over barn i barnehagen og i grunnopplæringen

Personvernet skal alltid veies opp mot andre interesser, rettigheter og samfunnsplikter. For at barn skal være sikret tilfredsstillende trygghet, helse, velferd og utdanning må registrering, lagring og utlevering av personopplysninger mellom ulike offentlige myndigheter finne sted. Det er imidlertid viktig å sikre at registrering og behandling av personopplysninger om barn er proporsjonalt med formålet.

I oktober 2007 sendte departementet på høring et forslag om å hjemle opprettelsen av en nasjonal database med opplysninger om barn i barnehagen. Formålet med registeret er oppgitt å være utarbeidelse av statistikk, forskning og analyse for å undersøke langsiktige effekter av deltagelse i barnehage i forhold til senere utdanning samt andre forhold som har betydning for sosial utjevning.

Datatilsynet var svært kritiske i sin høringsuttalelse og pekte blant annet på at det ikke er gitt nærmere regler for hvilke opplysninger registeret skal inneholde, hvem som skal ha tilgang, om det skal kunne kobles til andre registre etc. De hevder at Kunnskapsdepartementet har gitt en blankofullmakt til å opprette en nasjonal database som over tid vil komme til å omfatte tilnærmet hele befolkningen, ettersom de fleste barn i dag har kortere eller lengre tilknytning til en barnehage i løpet av sine første leveår.

Sommeren 2008 sendte Kunnskapsdepartementet på høring et forslag om etablering av et

sentralt register med opplysninger om elever i grunnskolen og videregående skole. Registeret skal inneholde en rekke personopplysninger, herunder opplysninger av svært sensitiv karakter. Registrering og behandling av personopplysninger skal gis hjemmel i lov ved endringer i opplæringsloven og privatskoleloven. Registeret skal være pseudonymt, slik at uvedkommende ikke skal kunne identifisere enkeltpersoner.

Formålet med et slikt register er å legge til rette for forskning som kan bidra til å bedre kvaliteten i norsk skole. Registeret skal generere kunnskap om læringsnivå og skoleeiers bruk av læringskompetanse og læringsutbytte. Departementet hevder at data som allerede samles inn, gjennom for eksempel elevundersøkelser og kartleggingsprøver, gir et for dårlig grunnlag til å tilrettelegge undervisning til enkeltelever og grupper på best mulig måte. Det pekes på at dagens data må suppleres med et «representativt og pålitelig datamaterialet fra grunnopplæringen, også på individnivå» (Kunnskapsdepartementet 2008).

Forslaget begrunnes blant annet med at myndighetene har ansvar for å legge forholdene til rette slik at offentlige og private skoleeiere kan arbeide for å bedre kvaliteten i skolen. Dette forutsetter at det finnes data som kan gi grunnlag for analyser, statistikk og forskning, og som kan brukes til kvalitetsutvikling og kvalitetskontroll. Dette innebærer også registrering av sensitive personopplysninger som kunnskap om helseforhold, seksuell legning, etnisk bakgrunn og religiøs oppfatning. Behovet for registrering av sensitive opplysninger begrunnes i at kvalitetsarbeid forutsetter kunnskaper om hvordan den enkelte opplever det fysiske og psykososiale læringsmiljøet, og at det er viktig for tilrettelegging av spesialundervisning og undervisning for utsatte grupper.

Det foreslås at alle skal være pliktig å gi fra seg personopplysningene, registrering skal altså ikke være basert på et samtykke fra den enkelte. Via en individuell kode skal det være mulig å følge enkeltindivider gjennom hele grunnopplæringen. Det skal også være mulig å koble registret mot andre registre, for eksempel i barnehagesektoren, jf. det tidligere nevnte barnehageregisteret. I sin høringsuttalelse peker Datatilsynet på at en kobling mot barnehageregisteret vil gjøre det mulig å følge enkeltpersoner over en 25-års periode, alt avhengig av studieprogresjon. Det påpekes at det foreslåtte registeret vil være det mest omfattende personopplysningsregisteret i Norge med hensyn til opplysningenes art, omfang og koblingsmuligheter (Datatilsynet 2008).

Departementet foreslår to alternativer for kvalitetssikring. Alternativ én innebærer at personopplysninger blir sjekket og kvalitetssikret før de blir pseudonymisert og lagret i det sentrale registeret. Det vil si at personidentifisere opplysninger blir lagret i en overgangsperiode. Alternativ to innebærer at kvalitetssikringen skjer etter at opplysningene er pseudonymisert. Dette alternativet vil medføre økt risiko for feil som kan videreføres til statistikk, forskning og analyser. Derfor forutsetter alternativ to at myndighetene kan kontakte skoleeier via pseudonymforvalter for å avdekke og korrigere feil. Det er imidlertid uklart hvilke opplysninger som skal registreres og hvem som skal samle dem inn.

Kommunesektorens interesse og arbeidsgiverorganisasjon (KS) sier i sin høringsuttalelse at de tviler på at personopplysninger på så aggregert nivå bidrar til en bedre opplæring.

Personvernkommisjonen er ikke overbevist om at et såpass omfattende register er nødvendig for å legge til rette for forskning som skal bidra til å heve kvaliteten i norsk skole. Forslaget inneholder ikke en tilfredsstillende risiko- eller konsekvensanalyse der personvernutfordringene er vurdert mot nytteverdien, sammenlignet med alternative metoder. Det er derfor vanskelig å vurdere om registeret er proporsjonalt med formålet. Når det gjelder forskningsformål er det per i dag mulig å innhente sensitive personopplysninger, men da i forbindelse med konkrete forskningsprosjekter og i samsvar med etablerte prosedyrer og rutiner. Når man knytter innsamlingen til et konkret formål, blir innsamlingen begrenset til det som er strengt nødvendig, noe som ivaretar sentrale personvernprinsipper som minimalitet og formålsbestemthet.

Personvernkommisjonen stiller seg videre kritisk til at alle som mottar opplæring skal være pliktige til å gi fra seg sensitive personopplysninger. I den grad skolen trenger sensitive personopplysninger bør tilgangen til disse være basert på samtykke og tillit mellom foreldre, elever og skolen. Kommisjonen mener også at det er uheldig at det foreslåtte registeret ikke bare vil omhandle opplysninger som angår barnet selv, men også barnets familie. Religiøs tilknytning er en sensitiv personopplysning og oppfattes av mange som et rent personlig anliggende. I tillegg er det mange barn som kommer fra familier som bærer med seg en historie der spørsmål om religiøs tilhørighet absolutt ikke bør komme myndighetene i hende. Det bør stilles spørsmål ved eventuelle emosjonelle kostnader ved å måtte gi fra seg sensitive opplysninger av særlig privat karakter.

Personvernkommisjonen mener generelt at det er uheldig at det opprettes sentrale registre som inneholder så mye informasjon om enkeltpersoner gjennom hele barne- og ungdomstiden.

14.3.8 RFID-og GPS-sporing

Når vi tar i bruk ny teknologi er det lett å overskride grenser. En skole i Doncaster (UK) prøver ut bruk av RFID-brikker sydd inn i elevenes skoleuniformer for å spore hvor elevene til enhver tid befinner seg. Formålet med systemet oppgis å være å effektivisere arbeidet med å registrere tilstedeværelse og gi foreldrene økt trygghet ved at man til enhver tid vet hvor hver enkelt elev befinner seg (Williams 2007).

The Guardian melder om et lignende system basert på GPS-teknologi der foreldre kan gå inn på en nettside for å spore hvor barnet deres er, forutsatt at barnet bærer en jakke utstyrt med en GPS-basert sporingsenhet (Crace 2007).

I likhet med PC-overvåkning mener Personvernkommisjonen at denne formen for overvåkning er et stort inngrep i den enkeltes integritet og at både skoler, foreldre og ikke minst staten bør være bevisste i forhold til bruk av overvåkningsteknologi ovenfor barn, se drøftelsen ovenfor.

14.3.9 Personvern for førskolebarn

Mange barnehager har egne hjemmesider på nett, og i noen barnehager benytter personalet disse sidene til å publisere bilder av daglige aktiviteter i barnehagen (måltider, lek, utflukter, og lignende). Både tilgjengeligheten av rimelige digitalkameraer og enkle løsninger for nettpublisering har senket terskelen for slik bildebruk. Formålet kan være markedsføring av barnehagen, eller rett og slett at personalet synes at slike bilder er hyggelige og av den grunn ønsker å spre dem.

Også lokalaviser bringer fra tid til annen reportasjer fra barnehager som viser barn i daglige aktiviteter.

Det eksisterer imidlertid mulighet for at selv uskyldige bilder av barn på nett misbrukes. John Ståle Stamnes, politioverbetjent i Kripos, uttaler til Dagsavisen: «Når vi går gjennom beslag ser vi ofte at uskyldige barnebilder blir blandet sammen med fotografier som viser overgrep.» Videre opplyser Stamnes at pedofile også manipulerer vanlige bilder slik at barnet fremstår i noe som ser ut som et overgrep (Prestegården 2008).

Mange foreldre ønsker derfor ikke at bilder av deres barn skal publiseres på nett eller i aviser.

Et bilde der en person kan gjenkjennes er en personopplysning og i tillegg har åndsverkloven egne regler om retten til eget bilde (se kapittel 13.2.1 for en nærmere drøfting). Publisering av slike bilder, i aviser eller på Internett, krever derfor normalt samtykke fra den eller de som er avbildet. Personvernkommisjonen erfarer at kjennskapet til regelverket omkring bildebruk i aviser og på nett varierer, og at mange, inklusive ansatte i barnehagene, ikke kjenner til kravet om samtykke, eller har kunnskap om hvordan adgangen til bildene kan begrenses gjennom at nettsider utstyres med passordbeskyttelse og at bilder legges ut i så lav oppløsning at enkeltindivider ikke kan gjenkjennes. Personvernkommisjonen mener at utdanningen for barnehagepedagoger bør ta høyde for at digitale verktøy er på full fart inn i barnehagene, og at studentene derfor bør gis informasjon om personvern og opplæring i det å håndtere personvernproblemer knyttet til bruk av digitale verktøy.

14.4 Forslag til tiltak

14.4.1 Tiltak for å trygge barn og unges rettsikkerhet og personvern

Det er ingen tvil om at barn har rettigheter med hensyn til personvern, både etter nasjonal og internasjonal rett. Kommisjonens mener imidlertid å ha identifisert klare svakheter ved dagens rettslige regulering. Dette gjelder for eksempel i forhold til hvem som skal utøve rettigheten; foreldrene, barnet eller barnet og foreldrene i felleskap? Videre har vi identifisert svakheter i forhold til spørsmålet om samtykkekompetanse, særlig når det gjelder foreldrenes rett til å samtykke på vegne av barna til publisering av personopplysninger, selv om barnets rett til integritet og personvern kunne tilsi at slik publisering ikke fant sted. En annen utfordring er den usikkerheten som synes å råde hos de forvaltningsorganene som er satt til å forvalte spørsmål om håndtering av barns personopplysninger og deres interesser generelt.

Det største problemet er kanskje at regler om personvern og personopplysningsvern ikke er utarbeidet med tanke på barn og unges spesielle situasjon. De er av generell karakter, og det er få holdepunkter i forarbeider til lovene for hvordan disse reglene skal anvendes overfor den sårbare gruppen som barn og unge representerer. Dette skaper dårlig forutsigbarhet og tilgjenglighet for både barna og deres foreldre. Mye av denne usikkerheten bør avklares gjennom rettsreglene.

Med bakgrunn i det som er sagt ovenfor om barns og foreldres samtykkekompetanse, samt det problematiske i å overskue virkningen på sikt av å publisere personopplysninger, herunder bilder, om barn og unge på nettet, foreslår kommisjonen at det utredes nærmere om denne typen behandling av personopplysninger bør ilegges restriksjoner, slik at samtykke etter personopplysningsloven § 8 (eventuelt § 9) ikke utgjør en tilstrekkelig behandlingsgrunnlag. Publiseringen må således hjemles i et av lovens øvrige alternativ. Etter Personvernkommisjonens oppfatning er det naturlig at dette vurderes i forbindelse med den pågående revisjonen av personopplysningsloven.

14.4.2 Styrking av personvernet ved bruk av digitale media

I kapittel 13.5 foreslår Personvernkommisjonen flere tiltak som skal bidra til å styrke personvernet i forhold til mediene, og særlig når det gjelder såkalte «nye media». Disse forslagene berører i høyeste grad de problemstillingene kommisjonen har valgt å fokusere på når det gjelder barn og unge.

Ett av forslagene er at det utredes om det bør opprettes et eget organ som dels kan bidra til å utvikle gode etiske retningslinjer og dels respondere på og løse ulike konflikter knyttet til nettytringer. Ettersom saker som angår krenkelse på Internett og digital mobbing sjelden finner veien til domstolene, mener Personvernkommisjonen at det er behov for et lavterskeltilbud hvor publikum kan henvende seg når de føler seg krenket. Et slikt lavterskeltilbud er ikke tenkt å være et statlig sensurorgan, men et organ som kan stoppe visse former for krenkelser når de er et faktum (Galtung 2008, s. 6). Et slikt lavterskeltilbud vil være av særlig betydning for barn og unge. Barn og unge har ikke tilstrekkelige ressurser til å bringe aktuelle saker til domstolene selv, det er heller ikke alle som har foreldre som har tilstrekkelige ressurser til å gjøre dette.

Kommisjonen mener også at det vil være hensiktsmessig å utforme en egen medieansvarslov, slik Ytringsfrihetskommisjonen foreslo i 1999. En slik lov skal definere roller og fastslå ansvar for alle typer media, både tradisjonelle forhåndredigerte og nye elektroniske brukerstyrte media. Forslaget er utdypet i fem punkter i kapittel 13.5.1 om media og personvern. I hovedtrekk går forslaget ut på at ethvert medium skal ha et ansvarssubjekt som kan kontaktes i forbindelse med personvernkrenkelser og som kan gjøres rettlig ansvarlig dersom krenkelsen må bringes til domstolene.

En medieansvarslov vil kunne ha en forebyggende effekt i forhold til å publisere ytringer som er krenkende og som kan skade personers omdømme. Med tanke på at nettytringer nærmest er irreversible og vil kunne påvirke barn og unge i lang tid etter at de er fremsatt, er det viktig med tiltak som kan forebygge krenkende og skadelige ytringer på nettet. Et definert ansvarssubjekt vil også kunne føre til at regler som gjelder aldersgrenser og samtykke blir fulgt.

14.4.3 Personvernansvarlig i skolen

Personvernkommisjonen foreslår at hver skole har en ansatt med spesiell kunnskap om personvern og personopplysningsloven. For små kommuner med få elever på hver skole kan det være en ansatt i kommunen med særlig ansvar for personvern i skolesektoren. Mange kommuner har allerede et personvernombud. Kommisjonen ser likevel behov for en ressursperson med særlig ansvar for barn og unges personvern i skolen. Skolens personvernressurs kan ha som oppgave å bistå elever i å ivareta sine rettigheter, bistå i arbeidet med å skape gode rutiner for behandling av personopplysninger internt i virksomheten, påpeke brudd på regler om behandling av personopplysninger og holde seg orientert om utviklingen på personvernområdet. I tilegg kan en slik person gi råd og veiledning til elever, lærere og foreldre i spørsmål som angår personvern.

Ettersom flere av de personvernutfordringene som barn og unge står overfor er relatert til deres egen bruk av digitale media, kan skolen i samarbeid med elevene utarbeide etiske retningslinjer for bruk av Internett og digitale læringsplattformer.

I kapittel 18 om organisering av personvernmyndighetene foreslår kommisjonen å styrke personvernkompetansen i ulike sektorer. For ytterligere å styrke skolenes kompetanse på området, vil Personvernkommisjonen anbefale at spisskompetanse om personvernforhold bør finnes hos sentrale utdanningsmyndigheter, for eksempel hos Utdanningsdirektoratet. Direktoratet bør ha et overordnet ansvar for å kvalitetssikre digitale læringsplattformer og andre elektroniske læringsverktøy og gi råd til skolene og deres ressurspersoner om personvernsforhold, samt kunne reagere på og forhindre brudd på personvernet til elever der det forekommer.

14.4.4 Synlige etater på nettet

For barn og unge er nettet en viktig sosial arena. Vi har tidligere beskrevet hvordan nettsteder som Facebook, Nettby og Second Life blir flittig benyttet til sosialisering og samhandling.

Samfunnet forventer at offentlige etater som Datatilsynet og Barneombudet er tilgjengelig for publikum, slik at de kan drive informasjonsarbeide og veiledning. Det forventes videre tilstedeværelse av synlig politi på gater, torg og andre steder der mange mennesker ferdes, ikke bare for å drive med kriminalitetsbekjempelse, men også for å rettlede og veilede, og ikke minst gjennom synlighet, markere at politiet er tilgjengelig dersom publikum har bruk for assistanse.

Det finnes allerede noen enkeltstående eksempler på at offentlige etater er til stede på nettet ut over hjemmesider og e-postmottak. Kripos har for eksempel en «rød knapp». «Rød knapp» er et av 18 tiltak foreslått av det såkalte Faremo-utvalget (arbeidsgruppe satt ned av Regjeringen den 1. juni 2006 for å utrede forslag til tiltak som kan forebygge at barn utsettes for seksuelle overgrep i forbindelse med internettbruk). Knappen er merket «politi» og kan plasseres på enhver nettside. Knappen lenker til Kripos, og ved å trykke på knappen kommer man til tipsmottaket til nettstedet *tips.kripos.no* og kan gi tips til politiet om uønsket aktivitet på nettet. PST (Politiets sikkerhetstjeneste) har en egen profil på Facebook. PST-sjef Jørn Holme begrunner dette som følger:

> «Politiets sikkerhetstjeneste når i dag frem til langt flere gjennom Facebook enn gjennom <den flotte hjemmesiden> vi har. For å nå frem holder det ikke å lage kjedelige hjemmesider beregnet på oss fra femti og oppover.» (Digi.no 2008).

Personvernkommisjonen synes begge tiltakene representerer en god begynnelse, men at man ikke bør stoppe der. Synlig tilstedeværelse på sosiale nettarenaer som er populære blant barn og unge bør bli en del av etatenes informasjonsstrategi. Som et minimum burde etater med barn og unge som målgruppe være tilstede i form av egne profiler på Facebook og i Nettby, og ved at en avatar[1] kan kontaktes i Second Life. På denne måten kan etatene gjøre seg tilgjengelig slik at de som ønsker å benytte slike arenaer kan abonnere på informasjonsmateriale, og de vil også kunne involvere seg i veiledning og dialog med publikum gjennom kanalene som disse nettstedene stiller til rådighet.

Det må understrekes at poenget med en slik «virtuell» tilstedeværelse ikke skal være å drive med «spaning» eller «overvåkning», men at den skal være en naturlig del av etatenes publikumsrettede arbeide.

Personvernkommisjonen mener videre at etatetene gjennom en tydelig og synlig tilstedeværelse på nettets virtuelle og sosiale arenaer kan markere at de betrakter nettet som en del av samfunnet, noe som i seg selv er et viktig poeng å kommunisere til barn og unge.

Kommisjonen vil derfor oppfordre de nevnte etatene til å utrede hvordan virtuell tilstedeværelse på ymse sosiale arenaer på nettet kan integreres i etatenes informasjons- og veiledningsarbeide rettet mot barn og unge.

14.4.5 Opplysningsarbeid og annet holdningsskapende arbeid

Skolen har et ansvar når det gjelder å informere elevene om rettigheter og plikter knyttet til samfunnsmedlemskap. Dette gjelder også på områder som har å gjøre med personvern og bruk av teknologi og nettbasert kommunikasjon. Som nevnt tidligere, viser statistikk presentert i *Trygg bruk*-undersøkelsen at barn og unge har blitt mer bevisst med hensyn til personvern ved bruk av informasjonsteknologi. Personvernkommisjonen mener skolen har et særlig ansvar når det gjelder å formidle informasjon om rettigheter og plikter angående personvern og videre skape gode holdninger som kan ligge til grunn for moralsk forsvarlig bruk av den digitale dømmekraften. Myndighetene har en uttalt målsetning om å sørge for at alle barn får grunnleggende IKT kompetanse og at denne kompetansen blir likt fordelt. Skolen skal motvirke klasseskiller med hensyn til digital kompetanse. Skolen har også et ansvar for å bidra til at personvernet blir likt fordelt. Skolen må informere barn og unge om de rettighetene de selv har, og om hvilke plikter de har overfor andre. Dette kan også være en del av skole/hjem-samarbeidet.

14.4.6 Delta på arenaer der det er mulig å påvirke internasjonale regler

Mye av det som utfordrer barn og unges personvern kan ikke reguleres ved nasjonal lovgivning. Derfor er det viktig at norske myndigheter deltar

[1] Representasjon, legemliggjørelse; symbol eller bilde som brukes (f.eks. i chatteprogrammer på Internett eller i virtual reality) til å representere en person (Kilde: Store Norske Leksikon),

på arenaer der det er mulig å påvirke utviklingen av internasjonale regler. For å beskytte personvernet til barn og unge er det særlig viktig å arbeide for felles retningslinjer med hensyn til aldersgrenser og samtykke.

Kapittel 15
Personvern i arbeidslivet

15.1 Innledning og problemstilling

15.1.1 Utviklingstrekk

Både arbeidslivet og næringslivet preges av store endringer. Utvikling og bruk av ny teknologi, endrede konkurranseforhold, demografisk utvikling, økt utdanningsnivå samt globalisering og internasjonalisering er viktige faktorer. Personvernkommisjonen har notert seg at organiseringen av arbeidet og arbeidsformer endres, og da særlig som en følge av at informasjonsteknologien endrer arbeidsprosesser og -oppgaver. Dette har fått flere følger for arbeidslivet. Den enkelte arbeidstaker har fått mer ansvar og større autonomi, med en mer fleksibel arbeidshverdag. Arbeidstakerne blir også mer selvstendige, og den enkeltes kunnskap er ofte bedriftens viktigste produksjonsmiddel. På mange arbeidsplasser er skillet mellom eier og ansatt mer uklart enn tidligere, gjennom at ansatte for eksempel får eierposisjoner og opsjonsavtaler. Samtidig ser man at arbeidstakerne ofte er mindre knyttet til den enkelte arbeidsgiver og at det er lett å skifte arbeidssted. Kommisjonen har også observert en holdningsendring i arbeidslivet; både hos arbeidstakere og arbeidsgivere. Dette kommer vi nærmere tilbake til under kapittel 15.3. Samtidig har utviklingen åpnet opp for teknologi som muliggjør overvåkning og kontroll av ansatte i et helt annet omfang enn det man har sett tidligere. Personvernkommisjonen har valgt å fokusere på økt overvåkning i arbeidslivet som en hovedproblemstilling innenfor dette feltet.

Den teknologiske utviklingen gjør det svært enkelt å overvåke både ansatte, kunder og andre som kan relateres til en virksomhet. Slik overvåkning vil etter kommisjonens oppfatning nødvendigvis påvirke holdninger – både hos arbeidsgiver og arbeidstaker. I forhold til arbeidsgiver vil det faktum at det er teknologisk enkelt og ressursmessig rimelig å overvåke ansatte og andre, medføre at presset på ytterligere overvåkning øker. Jo mer man vet, jo bedre. Utviklingstrekkene i arbeidslivet gjør at man finner begrunnelser for økt overvåkning. Når det gjelder arbeidstakere ser kommisjonen en rekke farer ved økt overvåkning – alt fra at det kan være en grov krenkelse av ansattes integritet til at det fratar ansatte ansvar for egne handlinger. Hvorfor stjeler man ikke fra arbeidsgiver? Fordi man er overvåket og dermed vil bli oppdaget, eller fordi man er et lovlydig menneske som ikke stjeler – uavhengig av overvåkning eller ikke?

Som en konsekvens av den teknologiske utviklingen og at ny teknologi i utstrakt omfang tas i bruk, er det kommisjonens oppfatning at det genereres, registreres og lagres en økende mengde informasjon. Informasjonen – eller opplysningene – vil være både «personopplysninger» i henhold til personopplysningsloven og andre opplysningstyper som ikke faller inn under dette begrepet. Se mer om personopplysningsbegrepet i kapittel 4.5.3.

Økt informasjonsvolum i arbeidslivet i form av ulike former for elektroniske spor, kommunikasjonsdata, elektronisk lagrede virksomhetsopplysninger og opplysninger om ansatte, vil generelt innebære økt risiko for lekkasje av opplysninger til uvedkommende. Dette kan dreie seg om alt fra datatyveri og lekkasje av bedriftshemmeligheter til at opplysninger om ansatte kommer på avveie internt i bedriften. Uansett fører denne risikoen med seg et behov for bedriften til å overvåke og ha kontroll over systemene sine. Utviklingen fører altså med seg et *økt kontroll- og overvåkningsbehov*. Slik overvåkning og kontroll fra bedriftens side vil nødvendigvis også omfatte opplysninger som direkte eller indirekte kan knyttes til bedriftens ansatte. Økt informasjonsmengde fører også med seg *en risiko for økt spredning av informasjon* (personopplysninger og andre opplysninger), både ønsket og uønsket sådan.

Man ser også at økt informasjonsmengde vil kunne medføre en *økt fare for at opplysninger blir brukt til andre formål*; det vil si at opplysninger som opprinnelig er innhentet og lagret for et bestemt formål senere blir benyttet til andre formål som ikke nødvendigvis er forenlige med det opp-

rinnelige formålet. Et eksempel på dette er opplysninger om ansattes bruk av Internett på arbeidsplassen. Slik bruk vil automatisk generere data som kan lagres i logger for administrasjons- og sikkerhetsmessige formål. Dersom det oppstår en arbeidsrettslig konflikt mellom den ansatte og bedriften, finnes det flere eksempler på at arbeidsgiver ønsker å legge fram slike logger som bevis for domstolene, for å underbygge sin sak.

Kommisjonen mener det bør oppfordres til en prinsipiell debatt om bruk av overvåkningsteknologi i arbeidslivet generelt. Man vil få et kvalitativt annet samfunn dersom man alltid skal benytte de muligheter som ligger i tilgjengelig teknologi. Det er derfor kommisjonens oppfatning at man bør ha en prinsipiell og kontinuerlig debatt om bruk av teknologi i samfunnet og da særlig i arbeidslivet.

15.1.2 Personvernhensyn i norsk arbeidsliv

Arbeidslivet i Norge preges av et ønske om likevekt mellom partene. Det legges særlig vekt på at det er ønskelig med størst mulig grad av tillit mellom arbeidstaker og arbeidsgiver. Videre fremheves økt medarbeiderdeltakelse, større grad av ansvarliggjøring og personlig frihet som idealer. Virkemidler som fremheves for å oppnå disse idealene er god informasjon og kommunikasjon mellom ansatte og arbeidsgiver.

Et grunnleggende prinsipp er at alle har krav på en viss grad av personvern og privatliv også på jobb. Denne rettigheten må balanseres mot arbeidsgivers interesser når det gjelder å opprettholde effektivitet og beskytte seg mot skadelige konsekvenser av de ansattes handlinger.

Personvernkommisjonen har i kapittel 4.1 redegjort for det nærmere innholdet i personvernbegrepet. I dette kapittelet fremheves noen personvernprinsipper som er særlig sentrale innen arbeidslivet.

Det første er *prinsippet om medbestemmelse*. Prinsippet om medbestemmelse innebærer at den registrerte (her den ansatte) skal kunne delta i og ha en viss mulighet til å påvirke andres behandling av opplysninger om seg selv. I dette ligger det at den behandlingsansvarlige (her arbeidsgiver) skal sørge for at innsamlingen og bruken av personopplysninger er kjent, transparent og forståelige. Medbestemmelsesprinsippet viser seg gjennom regler som sikrer den registrertes rett til kontroll over egne opplysninger og oversikt over når og hvordan disse brukes. Viktige regler i så måte er for det første regler som oppstiller krav om den registrertes *samtykke* til behandling av opplysninger, se for eksempel personopplysningsloven § 8 og § 9. For det andre vil regler som oppstiller en rett til *innsyn* i opplysninger som behandles, sikre den ansatte oversikt og kontroll og gjennom dette medbestemmelsesrett over opplysninger om seg selv, se for eksempel personopplysningsloven § 18. For det tredje vil regler som sikrer at den ansatte får *informasjon* om bruk av personopplysninger sikre slik medbestemmelsesrett, se personopplysningsloven § 19. Disse reglene vil sikre god åpenhet og kjennskap til behandling og bruk av personopplysninger på arbeidsplassen. Dette vil igjen sikre forutberegnelighet og ivareta de ansattes rettssikkerhet.

Økt medarbeiderdeltakelse fremheves som et arbeidsrettslig ideal i Norge. Det personvernrettslige medbestemmelsesprinsippet ligger nært opp til dette idealet, men de to hensynene kan etter kommisjonens oppfatning ikke likestilles helt. Det arbeidsrettslige idealet om medarbeiderdeltakelse er mer en rett til å bli hørt og til å delta i prosesser, jf. for eksempel arbeidsmiljøloven § 9-2 om plikt til å drøfte kontrolltiltak. Men idealet og prinsippet om medbestemmelse har sin begrunnelse i både det arbeidsrettslige feltet og det personvernrettslige feltet.

Etter personopplysningsloven kan samtykke være en tilstrekkelig behandlingsgrunn, jf. personopplysningsloven § 11 jf. § 8 første alternativ og § 9, 1. ledd bokstav a, og i mange sammenhenger fremheves dette som den prinsipale, eller foretrukne, behandlingsgrunnen, se kapittel 7.1.1. Det er et vilkår at samtykket er frivillig og ikke avgis under noen form for tvang fra den behandlingsansvarlige. Fordi arbeidsgiver alltid har en viss makt over de ansatte gjennom sin styringsrett, vil det i noen situasjoner kunne stilles spørsmål ved om et samtykke fra en ansatt er avgitt frivillig. Det er en potensiell fare for at den ansatte har i bakhodet at det å ikke avgi et samtykke i den gitte situasjonen vil kunne få betydning for fremtiden – selv om arbeidsgiver ikke har til hensikt å utnytte opplysningene til skade for arbeidstaker. Samtykke vil derfor ikke alltid være tilstrekkelig behandlingsgrunn i arbeidsforhold.

Det samme må antas å følge av arbeidsmiljøloven, hvor samtykke ikke er nevnt som begrunnelse for iverksettelse av kontrolltiltak fra arbeidsgivers side, jf. arbeidsmiljøloven § 9-1 nr 1. Videre vises det til rapporten *Protection of Workers' Personal Data* (ILO 1997), hvor det fremgår at samtykke som hovedregel ikke er tilstrekkelig for narkotikatesting av ansatte. Se også klagesak 2005/06 i Personvernnemnda, hvor samtykke ikke ble an-

sett som tilstrekkelig behandlingsgrunn for rustesting av ansatte hos Securitas.

Det neste prinsippet Personvernkommisjonen ønsker å fremheve er prinsippet om at behandling av personopplysninger skal være *saklig begrunnet*. Saklighetsprinsippet innebærer at all behandling av personopplysninger skal skje for et utrykkelig angitt formål som er saklig begrunnet i virksomheten. I forhold til relasjonen arbeidsgiver og arbeidstaker innebærer prinsippet en skranke for arbeidsgivers rett til å samle inn og registrere opplysninger om ansatte. Videoovervåkning av lokaler hvor ansatte befinner seg kan i mange situasjoner være saklig begrunnet ut fra arbeidsgivers behov, for eksempel i virksomheter som er utsatt for ran. Videoovervåkning av selve de ansatte, og ikke kun lokalet, kan imidlertid raskt bli oppfattet som en krenkelse av de ansattes integritet. Et eksempel på dette fra norsk rett finner man i Rt 1991, s. 616 (*gatekjøkkenkjennelsen*), som omtales nærmere nedenfor.

Hensynet til *proporsjonalitet* anser kommisjonen som et viktig personvernrettslig prinsipp med stor relevans innen arbeidslivet. Proporsjonalitetsprinsippet gjør seg gjeldende på ulike måter. For det første stiller det krav om at det inngrep som behandlingen medfører i den enkeltes personlige integritet ikke skal være uforholdmessig i forhold til det formålet man ønsker å oppnå med behandlingen. Det setter videre krav om at de tiltakene som iverksettes skal stå i forhold til det problemet man har. I forhold til overvåkning på arbeidsplassen innebærer det at graden av overvåkning skal stå i forhold til det eller de problemene arbeidsgiver ønsker å løse. Dette tolker kommisjonen som et krav til iverksetting av adekvate, hensiktsmessige og effektive tiltak som de ansatte er informert om. Videre skal formålet søkes oppnådd på den minst inngripende måten.

Til sist nevnes hensynet til *kvalitet*. I den grad arbeidsgiver benytter personopplysninger til å treffe beslutninger om ansatte, for eksempel for fordeling av arbeidsoppgaver, og kanskje enda tydeligere ved ansettelser, forfremmelser og oppsigelser, er det viktig at informasjonsgrunnlaget arbeidsgiver benytter er korrekt. Kvalitetsprinsippet vil på samme måte som medbestemmelsesprinsippet omfatte regler som sikrer den registrertes rett til kontroll og oversikt over behandling av opplysninger om seg selv; regler om innsyn, informasjon, retting og sletting.

15.1.3 Aktuelle spørsmål

Personvernkommisjonen har i sitt arbeid valgt å se på overvåkning i arbeidslivet generelt, med arbeidsgivers rett til innsyn i ansattes e-post som ett eksempel. Vi har også sett på varslingsinstituttet selv om dette tematisk er noe annet enn overvåkning. Avslutningsvis har vi valgt å si noe om den rettslige plasseringen av regelverket. De to første punktene gir etter kommisjonens oppfatning et godt bilde av de utfordringene som oppstår i interesseavveiningen mellom arbeidsgivers og arbeidstakeres interesser.

Etter kommisjonens mening vil en av utfordringene på dette område være å trekke en hensiktsmessig grense mellom «sikkerhetstiltak» og «overvåkningstiltak». Sikkerhetstiltak vil ofte være tiltak som iverksettes for å begrense faren for at arbeidstaker gjør feil som får konsekvenser for tredjeparter. Det vil ofte være bedriftens ytre sikkerhet som er viktig. Sikkerhetstiltak vil være tiltak som bedriften har en legitim interesse i å iverksette og det vil her være et relativt vidt spillerom for bedriften. Grensen vil imidlertid være en annen for tiltak som kan betegnes som «overvåkningstiltak». Noen overvåkningstiltak vil være legitime og kan være med på å bedre trygghetsopplevelsen i yrker som innebærer fare, for eksempel risiko for ran. Men dersom overvåkningstiltak er iverksatt på bakgrunn av mistillit mot arbeidstakere, vil overvåkningen være et uttrykk for mistillit og manglende respekt og kunne oppleves som belastende og stressende for arbeidstaker. Skillet mellom sikkerhetstiltak og overvåkningstiltak kan imidlertid på mange områder være glidende. Et tiltak som adgangskontroll til en bedrift vil kunne være både et sikkerhetstiltak og et overvåkningstiltak: Man sikrer seg at kun autorisert personale kommer inn i bygningen og at samtlige ansatte er ute av bygningen ved for eksempel brann. Samtidig kan adgangskontroll benyttes for å føre logg over hvem som er på jobb til hvilke tider og gjennom dette overvåke ansattes arbeidsinnsats.

En annen utfordring er å trekke en hensiktsmessig grense mellom privat informasjon og virksomhetsrelatert informasjon. En ytterligere problemstilling er skillet mellom arbeidstid og fritid.

15.2 Rettslig regulering på området

I rapportens del II finnes en grundig redegjørelse av personvernets rettslige regulering. Her foretas bare en kort gjennomgang av bestemmelser og

avgjørelser som er særlig aktuelle på arbeidslivets område.

Grunnloven inneholder enkelte bestemmelser som vil være relevante for ansattes integritetsvern på arbeidsplassen. Grunnloven § 100 om ytringsfrihet gjelder også på arbeidslivets område. I utredning fra Arbeidslivslovutvalget (NOU 2004:5) utrykkes dette slik:

> «Den ansatte omfattes av det samme ytringsfrihetsvernet som enhver annen borger. Ytringsfriheten er nedfelt i Grunnloven § 100. Bestemmelsen uttrykker et allment prinsipp som er begrunnet i tungtveiende samfunnsmessige hensyn.»

EMK artikkel 8 og SP artikkel 17 om respekt for hjem og privatliv får også betydning på arbeidslivets område. Det er etter avgjørelser fra EMD klart at EMK artikkel 8 oppstiller et vern som omfatter også kontorlokaler og gjennom dette gir et vern for ansattes personlige integritet på arbeidsplassen, se *Niemietz mot Tyskland* (dom 1992-12-16), som er omtalt nærmere nedenfor.

Straffelovens bestemmelse i § 390 om vern av privatlivets fred mot offentlig meddelelse om personlige eller huslige forhold, vil innbefatte et vern også for arbeidstakere mot at arbeidsgiver offentliggjør opplysninger vedkommende har kjennskap til i egenskap av å være arbeidsgiver.

Arbeidsmiljøloven har regler som verner arbeidstakeres personlige integritet på arbeidsplassen. Disse bestemmelsene innebærer dermed en begrensing i arbeidsgivers styringsrett. Arbeidsmiljøloven kapittel 9 oppstiller regler om kontroll i arbeidslivet. Lovens § 9-1 bestemmer at

> «[a]rbeidsgiver kan bare iverksette kontrolltiltak overfor arbeidstaker når tiltaket har saklig grunn i virksomhetens forhold og det ikke innebærer en uforholdsmessig belastning for arbeidstakeren.»

Videre slås det fast at personopplysningsloven gjelder for arbeidsgivers behandling av opplysninger om arbeidstakere i forbindelse med kontrolltiltak med mindre annet er fastsatt i lov. Plikt til drøfting, informasjon og evaluering av kontrolltiltak fastsettes i § 9-2. Lovens § 9-3 og § 9-4 regulerer retten til innhenting av helseopplysninger om ansatte og når medisinske undersøkelser av arbeidssøkere og arbeidstakere kan kreves. Lovens kapittel 9 er nytt og kom inn i arbeidsmiljøloven av 2005. Tidligere har slike kontrolltiltak i arbeidslivet i det vesentlige vært regulert av ulovfestede arbeidsrettslige og personvernrettslige regler og prinsipper. Personopplysningsloven regulerer for eksempel et kontrolltiltak som fjernsynsovervåkning på arbeidsplassen. Arbeidsmiljøloven kapittel 9 suppleres i tillegg av både lovfestet og ulovfestede arbeidsrettslige og personvernrettslige regler. Dette omhandles nærmere nedenfor.

Arbeidsmiljøloven kapittel 13 om vern mot diskriminering kan også sies å være regler som innebærer en viss grad av beskyttelse av ansattes integritet på arbeidsplassen, selv om de i utgangspunktet er ment å verne mot diskriminering på grunnlag av politisk syn, medlemskap i arbeidstakerorganisasjon, seksuell orientering, funksjonshemming og alder, se § 13-1. Opplysninger om slike forhold skal ikke medføre usaklig forskjellsbehandling.

Tilsvarende vern på grunnlag av kjønn oppstilles i likestillingsloven og i diskrimineringsloven ved diskriminering på grunn av etnisitet, nasjonal opprinnelse, avstamming, hudfarge, språk, religion og livssyn.

De generelle reglene som oppstiller et personvern for ansatte eksisterer parallelt med særlige regler som innskrenker eller gjør inngrep i ansattes personlige integritet. Regler som forplikter ansatte til å delta i regelmessige helseundersøkelser (eksempelvis luftfartsloven § 5-3 med forskrift[1]) eller avgi blodprøve ved mistanke om bruk av rusmidler (eksempelvis luftfartsloven § 6-11 og helsepersonelloven § 8) er bestemmelser som innebærer et inngrep i den ansattes personlige integritet, men hvor man har funnet at andre hensyn veier tyngre enn hensynet til den ansattes personvern.

For enkelte yrker må man legge fram politiattest, og særlig gjelder dette for personer som skal jobbe med barn eller unge. Eksempelvis er det hjemmel for å kreve politiattest i forbindelse med ansettelse i barneverntjenesten eller i barnevernинstitusjoner (se barnevernloven § 6-10), ved ansettelse i barnehager (se barnehageloven § 19), grunnskolen og den videregående skolen (se opplærngsloven § 10-9) og fra ansatte i helsetjenesten som jobber med mindreårige eller personvern med utviklingshemming (se helsepersonelloven § 20a). Et annet eksempel finner vi i domstolsloven § 219 som hjemler krav om politiattest for personer som skal yte rettshjelp, herunder advokater. Nærmere regler om innhenting og bruk av politi-

[1] Se forskrift om generelle bestemmelser om utstedelse av luftfartssertifikater (BSL C 1-1a), kapittel 7.1.5 (politiattest) og kapittel 7.1.6 (legeattest).

attester finnes i strafferegistreringsforskriftens § 12 flg.

Utgangspunktet er likevel klart. Det er etter norsk og internasjonal rett ikke tvil om at ansatte har krav på vern av sin personlige sfære, også på arbeidsplassen. Dette utgangspunktet er også slått fast i prinsippavgjørelser fra Høyesterett.

I Rt 1991, s. 616 (*gatekjøkkenkjennelsen*) avviste Høyesterett fremleggelse av et hemmelig videoopptak fra en arbeidsplass som bevis i en arbeidstvist.

> «De ansatte på gatekjøkkenet var klar over at det var montert videokamera i lokalet. Formålet, som ble kommunisert til de ansatte, var å gjøre det mulig å oppholde seg på pauserommet og samtidig ha kontroll med om det kom kunder inn i forretningslokalet. At kameraet i perioder ble brukt til løpende overvåkning av de ansatte var ikke kjent og derfor i strid med forutsetningene for ordningen. Beviset var dermed innhentet ved hemmelig videoopptak. Høyesterett fremhevet at slik hemmelig overvåkning representerte et vidtgående integritetsinngrep i forhold til de ansatte og at fremgangsmåten medførte et slikt inngrep i den personlige integritet at den ut fra alminnelige personvernhensyn måtte ansees uakseptabel.»

Andre aktuelle avgjørelser finnes i Rt 2002, s. 1572 (*urmakerkjennelsen*) og RG 2002, s. 162. I sistnevnte sak tillot retten bevis innhentet ved skjult videoovervåkning. Retten mente at videoopptakene representerte et inngrep i personvernet som måtte tåles i et rettssamfunn og at de derfor heller ikke burde avskjæres som bevis. Motsatt i *tippekassekjennelsen* inntatt i Rt 2001, s. 668. Se også RG 1993, s. 77.

Det samme utgangspunktet om retten til en personlig sfære på arbeidsplassen er også slått fast av den Europeiske Menneskerettighetsdomstol (EMD), i medhold av den Europeiske Menneskerettighetskonvensjon (EMK) artikkel 8. Bestemmelsen fastsetter at enhver «har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse» (artikkel 8 punkt 1) og «privatliv» og «korrespondanse» er av domstolen tolket slik at det også omfatter en persons aktiviteter på arbeidsplassen. Sentrale avgjørelser er sakene *Niemietz mot Tyskland* (dom 1992-12-16) og *Halford mot Storbritannia* (dom 1997-06-25).

I Niemietz-saken hadde offentlig myndigheter gjennomsøkt klagers kontor, noe klager anførte at krenket hans rett etter EMK artikkel 8. Myndighetene på sin side anførte at artikkel 8 ikke ga beskyttelse mot gjennomsøking av en persons kontor, på bakgrunn av konvensjonens skille mellom privatliv og hjem på den ene siden og arbeidsliv på den andre. Myndighetene ble ikke hørt med dette. EMD fremholdt at det ikke var grunnlag for å tolke «privatliv» så snevert at det utelukket aktiviteter på arbeidsplassen.

I Halford-saken fant EMD at kontroll av telefonsamtaler som ansatte fører på arbeidsplassen var en overtredelse av konvensjonens artikkel 8. Halford var ansatt i politiet, og hadde adgang til to telefoner, hvor den ene kunne brukes til private formål. Det var ikke gitt noen restriksjoner eller instruksjoner om bruken av telefonene. Halford påsto at arbeidsgiver hadde avlyttet hennes telefoner med det formål å sikre seg bevis i en pågående tvist. EMD fant det klart at telefonsamtaler tatt fra kontorlokaler faller inn under «privatliv» og «korrespondanse» i artikkel 8.

En nyere avgjørelse fra EMD omhandler e-post og annen korrespondanse mer direkte. I saken *Copland mot UK* (dom 2007-04-03) stadfester EMD at e-post og trafikkdata knyttet til bruk av arbeidsgivers utstyr og Internett til personlige forhold er gitt samme beskyttelse etter EMK artikkel 8 som bruk av tradisjonelle kommunikasjonsformer, som for eksempel telefon.

I denne saken var klager ansatt som assistent for en rektor ved en skole i Wales. Skolens assisterende rektor hadde iverksatt overvåkning av klagers bruk av telefon, e-post og Internett fordi man mistenkte at klager brukte skolens utstyr til personlige formål utover det som var akseptert. Klager anførte at retten til privatliv og korrespondanse etter EMK artikkel 8 var krenket. EMD slo fast, under henvisning til tidligere praksis, at telefonsamtaler til og fra arbeidsplassen i utgangspunktet er omfattet av begrepene «privatliv» og «korrespondanse», jf. EMK artikkel 8 første ledd. Domstolen slo videre fast at e-post sendt til og fra arbeidsplassen og informasjon fra overvåkning av ansattes personlige bruk av Internett naturlig kan sammenlignes med bruk av telefon, og følgelig er omfattet av vernet gitt i EMK artikkel 8 første ledd. Klager hadde ikke fått noen informasjon om at vedkommende ville bli utsatt for overvåkning, og hadde dermed en rettmessig rimelig forventning om at telefon, e-post kommunikasjon og bruk av Internett var privat og ikke kjent for andre. EMD fant at innhenting og lagring av informasjon om klagers bruk av telefon, e-post og Internett, uten at vedkommende var gitt informasjon om det, innebar et inngrep i klagers rett til privatliv og korrespondanse etter EMK artikkel 8 første ledd.

Domstolen foretok så en vurdering av om inngrepet kunne anses å være «i samsvar med loven», jf. EMK artikkel 8 annet ledd. Staten anførte at skolen, som en offentlig institusjon etablert med hjemmel i lov, hadde hjemmel til å føre rimelig kontroll med at skolens utstyr ikke ble brukt til personlige formål utover det som var innenfor det akseptable. De argumenterte med at skolens utstyr var finansiert ved offentlige midler, og at det derfor var nødvendig med en viss kontroll for å sikre at skolen var i stand til å utføre sine lovbestemte oppgaver. Domstolen godtok ikke statens anførsler, og påpekte at staten ikke kunne vise til at det på tidspunktet da overvåkningen fant sted forelå hjemler, verken i nasjonal lovgivning eller i skolens reglement, som ga arbeidsgiver adgang til å overvåke arbeidstakers telefon, e-post eller bruk av Internett. Ettersom det på det aktuelle tidspunktet ikke forelå nasjonal lovgivning som hjemlet slik overvåkning, var inngrepet etter artikkel 8 første ledd ikke «i samsvar med loven», jf. artikkel 8 annet ledd.

Domstolen ville imidlertid ikke utelukke at overvåkning av en arbeidstakers telefon, e-post eller bruk av Internett på arbeidsplassen i visse situasjoner kunne være «nødvendig i et demokratisk samfunn» for å oppnå et legitimt formål, men ettersom lovskravet i artikkel 8 annet ledd uansett ikke var oppfylt, var det ikke nødvendig å ta stilling til dette i den konkrete saken.

Den internasjonale arbeidsorganisasjonen ILO (International Labour Organisation) har utarbeidet en adferdskodeks for beskyttelse av personopplysninger om arbeidstagere; *Protection of Workers' Personal Data* (ILO 1997). Dette er veiledende retningslinjer om anbefalt praksis ved utarbeidelse av lovgivning, kollektive avtaler og ved behandling av personopplysninger om arbeidstakere. Retningslinjene omhandler også konkrete anbefalinger vedrørende narkotikatesting av ansatte, diskriminering og personlighetstesting.

15.3 Teknologiske utviklingstrekk som kan true personvernprinsippene

Idealene i arbeidslivet i Norge er ovenfor beskrevet med stikkordene tillit, økt medarbeiderdeltakelse, større grad av ansvarliggjøring og personlig frihet. Virkemidlene som fremheves er informasjon og kommunikasjon mellom partene. De personvernrettslige prinsippene som særlig fremheves som viktige i forhold til ivaretakelse av personvern og personlig integritet på arbeidsplassen er prinsippet om *medbestemmelse*, *saklighetsprinsippet* og *proporsjonalitetsprinsippet*. Personvernkommisjonen ser at den teknologiske utviklingen i arbeidslivet utfordrer en rekke av disse prinsippene.

Den teknologiske utviklingen gir økte muligheter for registrering av opplysninger og gjennom dette overvåkning og kontroll av ansatte. Måten arbeidslivet er innrettet og organisert på i dagens samfunn medfører at det registreres flere opplysninger, også personopplysninger. Dette kan være opplysninger som har form av data (for eksempel elektroniske spor) eller opplysninger som klart er av personlig art (for eksempel opplysninger sendt mellom venner i en e-post). Omfanget og mengden opplysninger som automatisk genereres og lagres om ansatte er i seg selv en utfordring i forhold til for eksempel forholdsmessighetsprinsippet og proporsjonalitetsprinsippet.

Som en følge av den teknologiske utviklingen ser man også en sammenblanding mellom privatlivet og arbeidslivet. Denne sammenblandingen mellom jobb og fritid gjør det vanskelig å opprettholde skillene man til nå har hatt mellom arbeid og fritid.

Mange arbeidstakere forventes å være tilgjengelig for arbeidsgiver til enhver tid, samtidig som teknologien gjør det mulig å jobbe hjemme eller utenfor kontoret døgnet rundt. Arbeidshverdagen spiser mer og mer av fritiden. Den andre siden av denne utviklingen er imidlertid at arbeidstakerne i økende grad tar for seg av arbeidsgivers tid og ressurser, og da særlig i form av at private gjøremål utføres i det som kan betegnes som arbeidets kjernetid. Ansatte benytter bedriftens utstyr og ressurser til private formål, for eksempel til å kommunisere privat, enten via telefon, mobiltelefon, e-post eller på andre måter.

Dette har blitt betegnet som en utvikling hvor ansatte tiltar seg et privatliv på arbeidsplassen og hvor arbeidslivet flytter hjem til folk – en privatisering av arbeidshverdagen og vice versa. Man ser en holdningsendring når det gjelder respekten for arbeidsgivers og arbeidstakers tid og ressurser. Teknologien gjør det enklere for den enkelte å ta for seg av arbeidsgivers tid, ressurser og verdier, uten at dette oppdages. Følgelig blir overvåkningsbehovet fra arbeidsgivers side mer påtrengende.

I forlengelsen av denne utviklingen har det oppstått et spenningsfelt med hensyn til hvilken rett arbeidsgiver har til å foreta innsyn i elektronisk lagrede data på sitt utstyr, for eksempel e-post og dokumenter som den ansatte har lagret på

sin datamaskin. Enkelte betegner dette som «snoking» i private opplysninger, mens andre mener at arbeidsgiver har rett til å foreta innsyn i informasjon og dokumentasjon som ligger på arbeidsgivers utstyr og nettverk.

Interessemotsetningene mellom arbeidsgiver på den ene siden og arbeidstaker på den annen har i forhold til denne problemstillingen særlig kommet på spissen i spørsmålet om fremleggelse av dokumentbevis i arbeidsrettstvister. Arbeidsgiver har ønsket å legge fram utskrifter av e-post eller andre former for korrespondanse som bevis for å underbygge sin sak. Arbeidstakers oppfatning er at dokumentbeviset er ulovlig ervervet, med henvisning til personvernet. Enkelte har i forlengelsen av slike saker argumentert for at dokumentasjonsbehovet i arbeidsrettslige tvister vil legge føringer på overvåkningsbehovet til arbeidsgiver. Jo strengere, mer komplisert og omfattende dokumentasjonskravet praktiseres, jo større behov vil arbeidsgiver ha for overvåkning. Slik overvåkning vil ofte skje i det skjulte og dermed utfordres både medbestemmelsesprinsippet og muligheten ansatte har til å kontrollere om tiltak som iverksettes er proporsjonale i forhold til det som ønskes oppnådd.

Elektroniske søkemotorer på Internett gjør det enkelt å finne opplysninger om arbeidssøkere og arbeidstakere. Såkalt «googling» av arbeidssøkere og ansatte har blitt mer og mer vanlig. Slik informasjonsinnhenting fra arbeidsgivers side er helt klart en utfordring for arbeidssøkere og ansattes personvern og setter etter kommisjonens oppfatning både medbestemmelsesprinsippet og saklighetsprinsippet på prøve.

Enkelte har anført at det ikke er den teknologiske utviklingen som sådan som er problemet, men at det er bruken av teknologien som er utfordringen. Tanken er da at «teknologien er nøytral» og at det er vår bruk av teknologien som skaper trusselen.

Personvernkommisjonen er usikker på om den er enig i en slik påstand. Etter kommisjonens oppfatning er *utbredelsen* av teknologien i seg selv en utfordring. Summen er betydelig og man kan ikke vurdere teknologien som nøytral uten å ta hensyn til hvilket omfang teknologien har.

Et annet moment er at økt grad av tilgjengelige tekniske hjelpemidler i seg selv gjør at man tar i bruk nye tjenester og tilbud og slik utnytter teknologien. Det er kommisjonens oppfatning at tilgjengeligheten av slik teknologi på enkelte områder vil påvirke omfanget av behandling av for eksempel personopplysninger som skjer i systemene. Det er nærliggende her å peke på hvordan skattelistene brukes i Norge, se kapittel 13.4.1.

15.4 Kommisjonens observasjoner og tilrådninger

15.4.1 Generelle betraktninger

Personvernkommisjonen gjennomførte et åpent seminar om personvern i arbeidslivet den 10. april 2008, hvor temaene var arbeidsgivers rett til innsyn i e-post og elektroniske dokumenter, varslingsreglene og overvåkning i arbeidslivet generelt.

Etter kommisjonens oppfatning gir det eksisterende regelverket på arbeidslivets område et relativt balansert vern for arbeidstakere. På enkelte områder ser imidlertid kommisjonen et behov for forbedringer og tiltak. Kommisjonen har valgt å fokusere på to hovedområder; arbeidsgivers tilgang til e-post og elektroniske dokumenter hos de ansatte samt varslingsreglene. Kommisjonen erfarer også at det er et problem at reglene for personvern og integritetsvern i arbeidslivet er spredt over forskjellige lover og rettsområder. Dette er en utfordring i forhold til følelsen av «eierskap til regelverket», noe som igjen får konsekvenser for etterlevelsen av det gjeldende regelverket. Kommisjonen vil derfor kommentere dette forholdet særskilt.

Nivået og omfanget av overvåkning i arbeidslivet synes å ha økt betydelig de siste årene. Tilgjengeligheten av ny teknologi forbundet med lave kostnader gjør terskelen lav for iverksetting av systemer som direkte eller indirekte kan sies å innebære kontrolltiltak overfor ansatte. Det kan være alt fra adgangskontroll til avlytting av telefonsamtaler og kartlegging av ansattes nettverk. Det har også blitt vanligere at private aktører tar i bruk «politimetoder» for å avdekke mislighold blant egne ansatte. Eksempler på dette er bruk av skjult kameraovervåkning og fremleggelse av bilder fra overvåkning som bevis mot arbeidstakere. Det er også eksempler på at arbeidsgiver har gått gjennom ansattes tekstmeldinger for å avdekke uønsket aktivitet i arbeidstiden (Datatilsynet 2006, s. 26f).

Det å bli overvåket i sitt daglige virke vil av de fleste oppfattes som en belastning. Dersom opplysningene som innhentes ved slik overvåkning i tillegg blir brukt til andre formål enn de opprinnelig var beregnet for, og andre formål enn dem man har fått informasjon om, øker dette belastnin-

gen og følelsen av overtramp mot den personlige integritet.

Personvernkommisjonen vil fremheve følgende grunnleggende retningslinjer for overvåkning på arbeidsplassen:

1. De ansatte skal være informert om at overvåkning finner sted, hvordan overvåkning skjer og til hvilke(t) formål.
2. Ansatte skal få informasjon om eventuelt endrede formål med overvåkningen.
3. Overvåkningen skal være nødvendig og arbeidsgiver skal ha vurdert om andre metoder ville vært tilstrekkelig eller mer hensiktsmessig.
4. Behandlingen av personopplysninger som følge av overvåkning skal oppfattes som rimelig av de ansatte.
5. Graden av overvåkning skal stå i forhold til problemene man ønsker å løse (proporsjonalitetsprinsippet) og være saklig i forhold til den virksomheten som drives.

15.4.2 Innsyn i e-post og elektroniske dokumenter

Under det åpne seminaret opplevde kommisjonen at spørsmålet om arbeidsgivers rett til innsyn i e-post og elektronisk lagret informasjon på ansattes datamaskin og lagringsområder engasjerer mange.

Informasjon, åpenhet og gjennom dette forutsigbarhet for begge parter ble fremhevet som svært viktig. Man anerkjenner at det er uheldig for arbeidstaker at han eller hun ikke har informasjon om tiltak som iverksettes av arbeidsgiver, samtidig som det er viktig å se at arbeidsgiver kan ha en legitim interesse/behov for innsyn og kontroll. Det ble imidlertid fremhevet som uheldig dersom regelverket blir for ensidig i favør av arbeidstaker, blant annet fordi et *for* sterkt rettslig vern kan gi de ansatte falske forhåpninger, slik at de innretter seg på feil grunnlag.

Kommisjonen opplever at manglende bevisstgjøring er et problem hos begge parter – både arbeidstaker og arbeidsgiver. En prosess hvor begge parter gjøres oppmerksom på de utfordringer man står overfor er derfor nødvendig: behandling av personopplysninger i bedrifter og organisasjoner må synliggjøres. Det må gjøres klart hva som registreres av opplysninger, hva opplysningene brukes til og hvem som får tilgang til opplysningene.

I juni 2008 fremmet Justisdepartementet et lovforslag hvor det gis hjemmel i personopplysningsloven til å utarbeide forskrifter om arbeidsgivers rett til innsyn i ansattes e-post (Ot.prp. nr. 71(2007-2008)). Det foreslås også en ny bestemmelse i arbeidsmiljøloven kapittel 9 hvor det presiseres at arbeidsgivers innsyn i e-post reguleres av personopplysningsloven med forskrifter. Lovforslaget er p.t. ikke vedtatt.

Selve forskriften har vært på høring og er utarbeidet av Fornyings- og administrasjonsdepartementet som har fått delegert denne oppgaven. Forskriftens endelige utforming er ikke kjent i skrivende stund, da departementet avventer lovhjemmelen.

I følge høringsbrevet fra Fornyings- og administrasjonsdepartementet (FAD 2006) var det behov for en avklaring av rettstilstanden på dette området, da grensen mellom lovlig og ulovlig innsyn ble opplevd som uklar av både arbeidsgivere og arbeidstakere.

Forskriften, slik den fremstår i høringsutkastet, omhandler arbeidsgivers rett til innsyn i ansattes e-post, men reglene gjelder også innsyn i annen elektronisk kommunikasjon, internettbruk og private filer.

Reglene foreslås å komme til anvendelse også for andre enn typisk ansatte, for eksempel elever, studenter og engasjerte i frivillige organisasjoner.

Forskriftene tar utgangspunkt i at arbeidsgivere bare har rett til innsyn i ansattes e-post mv. når det er nødvendig for virksomhetens daglige drift eller for å ivareta andre berettigede interesser ved virksomheten, ved begrunnet mistanke om at e-postkassen inneholder opplysninger om straffbare forhold, eller ved begrunnet mistanke om at arbeidstakers bruk av e-postkassen medfører grovt brudd på de plikter som følger av arbeidsforholdet.

Forskriften søker altså å veie arbeidsgivers og arbeidstakers behov opp mot hverandre. Hovedregelen er imidlertid at arbeidsgiver *ikke* har innsynsrett i den ansattes personlige e-postkasse, definert som en e-postkasse som er knyttet til en bestemt persons navn eller som etter avtale skal være personlig.

Selv om den endelige e-postforskriften ikke foreligger, ønsker Personvernkommisjonen å knytte noen kommentarer til forslaget.

Personvernkommisjonen mener at plasseringen av disse reglene vil skape utfordringer i praksis. Etter kommisjonens oppfatning bør regler for innsyn i og kontroll av e-post og dokumenter legges til partenes lov; nemlig arbeidsmiljøloven, alternativt i en egen personvernlov for arbeidslivet. Det er nærliggende å tro at partene i arbeidslivet har størst kjennskap til sine særlover, og at spesi-

elle regler i en forskrift til den allerede generelle personopplysningsloven gjør disse mindre tilgjengelige for dem reglene retter seg mot. I denne forbindelse mener kommisjonen at det også er uheldig å sammenblande arbeidsplasser, skoler og universiteter samt frivillige og tillitsvalgte i foreninger og organisasjoner. Dette gjør bestemmelsene mer uoversiktlige.

I denne forbindelse vil Personvernkommisjonen presisere at vår kritikk av plasseringen ikke er relatert til at ikke andre grupper kan ha behov for vern mot uberettiget innsyn i elektronisk kommunikasjon. Det bør også eksistere regler som ivaretar personvernet til både skolelever og personer som jobber på mer frivillig basis. På grunn av de spesielle hensyn som gjør seg gjeldende i arbeidslivet, hvor både arbeidsgivers og arbeidstakers behov skal vektlegges, er det imidlertid viktig å se på arbeidslivet spesielt. Av hensynet til notoritet og tilgjengelighet er det dessuten av betydning at reglene forankres i arbeidsrettens regelverk.

Et annet aspekt som ikke er tilfredsstillende løst i forslaget er hensynet til tredjepersoner. Det er ikke bare den ansattes personvern som kan bli satt på prøve ved arbeidsgivers innsyn i korrespondanse. Den ansatte vil ofte ha kommunisert med tredjepersoner utenfor virksomheten. Hvilket vern skal avsender ha når mottaker av en e-post sitter som arbeidstaker i en bedrift? Og på hvilket rettslig grunnlag skal arbeidsgiver som behandlingsansvarlig pålegges et ansvar for slike utenforstående tredjeparter som bedriften ikke har oversikt eller kontroll over? På Kommisjonens åpne seminar om arbeidsliv og personvern opplyste Datatilsynet at regelverket for innsyn i e-post er ment å ha en «oppdragende effekt» på arbeidsgiver. Personvernkommisjonen vil bemerke at det er uheldig dersom det blir et for ensidig fokus på arbeidsgivers holdning i denne saken. Selv om maktfordelingen mellom arbeidsgiver og ansatt gjør at det først og fremst er behov for regelverk rettet mot arbeidsgiver, er det etter kommisjonens oppfatning viktig også å fokusere på ansattes holdning til kommunikasjon på arbeidsplassen og også ansattes bruk av arbeidsgivers tid og ressurser. Det bør ikke gjennom det eksisterende eller fremtidig regelverk skje en ensidig ansvarsplassering hos arbeidsgiver. Man bør gjennom regelverket søke å oppnå en «oppdragende effekt» av også de ansatte, ved å oppfordre til å ha et bevisst forhold til og ta ansvar for egne handlinger når det gjelder privat kommunikasjon og private gjøremål som utføres i arbeidstiden. På den måten vil den ansatte i stor grad selv kunne verne om sitt privatliv uten innsyn fra arbeidsgiver.

15.4.3 Varslingsreglene

I 2006 ble det vedtatt nye regler om varsling i arbeidslivet i arbeidsmiljøloven. Reglene har vært virksomme siden 01.01.2007.

Varsling er definert som de tilfeller der ansatte sier fra om kritikkverdige forhold på arbeidsplassen. Kritikkverdige forhold er forhold i strid med lov eller etiske normer, eksempelvis korrupsjon eller annen økonomisk kriminalitet, fare for pasienters liv og helse, farlige produkter eller dårlig arbeidsmiljø. Det er tale om varsling hvis arbeidstaker sier fra om slike forhold internt til ledelsen eller andre i virksomheten eller eksternt til blant annet tilsynsmyndigheter og media.

Etter de nye bestemmelsene er arbeidsgiver pliktig til å sørge for å legge til rette for et godt ytringsklima i virksomheten. Arbeidsgiver skal utarbeide rutiner for intern varsling eller sette i verk tiltak som legger forholdene til rette for intern varsling om kritikkverdige forhold i virksomheten. Det er videre gitt regler som skal verne arbeidstakeren (varsleren) mot gjengjeldelse fra arbeidsgiver, se arbeidsmiljøloven § 2-5.

Reglene er viktige for å sikre arbeidstakernes ytringsfrihet på arbeidsplassen og det er viktig at det etableres gode ordninger som verner de som varsler om kritikkverdige forhold. Det er imidlertid viktig også å være klar over at ordningen kan misbrukes. Det er viktig at personer det varsles om sikres en rettferdig og tillitvekkende prosess og at deres krav på personvern også ivaretas.

Et særskilt spørsmål er om vedkommende det varsles om skal få vite om varslingen. I en slik varslingsprosess vil det bli behandlet personopplysninger, og etter personopplysningsloven § 20 skal da vedkommende som hovedregel informeres. Problemstillingen kommer på spissen der varslingen er ubegrunnet, eller der varsling brukes som sjikane.

Anonym varsling er også en utfordring. Et særlig problem er forholdet til kontradiksjon; den det varsles om vet ikke hvem man kjemper i mot. Dette kan i noen tilfeller føre til misbruk av varslingsinstituttet. Retten til å varsle anonymt ivaretar varsleren, men ikke den det varsles om. Det er heller ikke mulig for bedriften å gi tilbakemelding til den anonyme varsleren om utfallet av en eventuell granskning, noe som i seg selv kan være uheldig.

Artikkel 29-gruppen har kommet med en uttalelse om varsling (Art 29 WP 2006a). De peker

her på flere forhold av betydning. For det første dataenes kvalitet og proporsjonalitet. For det andre peker de på viktigheten av å gi klar og utfyllende informasjon til de ansatte. For det tredje fremhever de som viktig å ivareta rettighetene til den det varsles om, ikke bare varsleren. For det fjerde peker de på behovet for tilfredsstillende sikkerhet rundt behandlingen av de opplysningene som kommer inn og behandles i forbindelse med varslingen. Og til sist, som et femte punkt, at det må utarbeides rutiner for varslingen.

Personvernkommisjonen mener man bør være klar over faren for trakassering og sjikane ved anonym varsling, men mener likevel at det som en sikkerhetsventil bør være mulig å varsle anonymt. Også her mener kommisjonen at åpenhet og tillit mellom partene må være et mål og at dette best kan nås gjennom tilrettelegging og informasjon til partene.

15.4.4 Rettslig plassering av reglene

Etter Personvernkommisjonens oppfatning er det et problem at reglene for personvern og integritetsvern i arbeidslivet er spredt over forskjellige lover og rettsområder. Reglene for arbeidstakeres integritetsvern (personvern og personopplysningsvern), arbeidstakeres ytringsfrihet, arbeidsgivers handlingsrom i forhold til behandling av opplysninger om ansatte eller opplysninger som kan knyttes til ansatte, er som nevnt nedfelt i både Grunnloven, arbeidsmiljøloven og personopplysningsloven med forskrifter.

Kommisjonen etterlyser derfor et helhetlig regelverk som tydelig angir grensene for arbeidssøkere og arbeidstakeres integritetsvern, personvern og personopplysningsvern. Løsningen man har valgt i Finland, hvor man har gitt en egen lov om personvern i arbeidslivet, bør etter kommisjonens oppfatning vurderes.

Lovgiver bør søke å få på plass et regelverk som partene i arbeidslivet er enige om, og hvor den nødvendige balansen mellom arbeidsgivers og arbeidstakers interesser er synliggjort. Et hensiktsmessig og godt balansert regelverk vil etter kommisjonens oppfatning være med på å sikre etterlevelse fra partenes side.

Den arbeidsrettslige reguleringen må sees i sammenheng med de forhold og regler som gjelder for næringslivet. En ensidig fokusering på arbeidstakeres rett til personvern og personopplysningsvern bør unngås. Det må etter kommisjonens oppfatning være et mål å få på plass et robust regelverk som tar høyde for den teknologiske utviklingen, endringer i arbeidslivet, økonomiske konjunkturer og arbeidslivets og næringslivets organisering og eierskap. Regelverket bør på best mulig måte ivareta både arbeidstakernes, virksomhetens og samfunnets behov. Et godt og forutsigbart regelverk samlet i én lov bør være målet.

Ved innføring av nytt og generelt arbeidsrettslig regelverk på området bør det gjøres obligatorisk å vurdere tiltakenes innvirkning på personvernet og personopplysningsvernet. Bestemmelsene om varsling er et eksempel på regelverk hvor man etter kommisjonens mening ikke har gjort tilfredsstillende utredning av personvern og personopplysningsvern og konsekvenser for de involverte partene.

Gjennom en tilfredsstillende vurdering av personvernrettslige konsekvenser, synliggjøres det hvilke vurderinger som er gjort, hvilke hensyn man har lagt vekt på og gjennom dette hvordan interesseavveiningen mellom personvernet og andre konkrete interesser faller ut. Dette vil gi et bedre grunnlag for å sikre en balansert interesseavveining i den videre praktisering av reglene. Balanse må etter kommisjonens oppfatning være et stikkord.

Kommisjonen ser det som særlig viktig at evaluering av og ivaretakelsen av *proporsjonalitetsprinsippet* kommer klarere fram i lovgivningsprosessen. Det er mange eksempler fra de siste årene på at behovet for endret eller ny lovgivning ikke på tilfredsstillende måte veies opp mot (eventuelle) negative effekter for ivaretakelsen av den personlige integritet og personvernet. Årsaken kan være at det ikke legges fram dokumentasjon eller materiale som gjør det mulig å gjøre en nærmere vurdering av hvilke effekter et lovforslag vil få for personvernet.

15.4.5 Andre tiltak som bør vurderes

Kommisjonen anbefaler at det iverksettes tiltak som øker bevisstheten rundt personvern i arbeidslivet, rettet både mot arbeidsgiversiden og arbeidstakersiden. Tiltakene bør ha som mål å ha en «oppdragende» effekt på både arbeidsgiver og arbeidstaker.

Eventuelle regelendringer og ny lovgivning bør skje etter en helhetlig avveining av mange motstridende og prinsipielle spørsmål. Kommisjonen oppfordrer til en prinsipiell diskusjon om *hva slags kultur, normer og retningslinjer* man ønsker i arbeidslivet for fremtiden. Et av spørsmålene som bør belyses i en slik debatt er hva som kan regnes

for å være akseptabel overvåkning. Et annet moment er hvor grensen for ansattes *berettigede forventning* til personvern og integritetsvern på arbeidsplassen kan eller bør gå. I hvilken grad kan den beskyttelsen i form av personvern som er gitt ansatte i dag sies å være «berettiget»? Og i hvilken grad kan den sies å egentlig beskytte ansatte? I forlengelsen av denne debatten vil det være nødvendig å se på utviskingen av grensene mellom arbeidstid og fritid.

Personvernkommisjonen anbefaler også at man får økt fokus på styrking av personvernkompetansen i arbeidslivet. I arbeidslivet finnes det allerede funksjoner som har til oppgave å ivareta de ansattes interesser, herunder arbeidstakernes fysiske og psykiske helse og velferd. Personvern og personopplysningsvern kan sies å være omfattet av dette. Verneombudet har en sentral rolle på de fleste arbeidsplasser, og Personvernkommisjonen mener det vil være hensiktmessig å presisere at verneombudets funksjon også omfatter personvernspørsmål, og derfor la temaet være en del av den opplæringen verneombudene er pålagt å gjennomføre.

Kapittel 16
Personvern i helsesektoren

Helsetjenesten er en viktig søyle i velferdsstaten og kan kort beskrives som statens organiserte innsats for å ivareta borgernes helsemessige behov. Helse er vidt definert og i denne sammenheng er det ikke nødvendig med noe skarpt skille mellom helsetjenester på den ene siden og sosiale tjenester og tilbud på den andre. Behandling, forebygging og avhjelping av sykdom, funksjonshemming og skade er sentrale oppgaver, som må løses i takt med samfunnsutviklingen.

Helsetjenesten skal løse mange oppgaver og er under et konstant press med tanke på både å gjøre mer (behandle flere), forbedre tjenestetilbudet (ta i bruk ny kunnskap og nye metoder, øke kvaliteten, fremme sikkerheten) og sørge for at tjenestene er kostnadseffektive. Helsetjenesten er avhengig av tilgang på helseopplysninger for å kunne gi pasientene forsvarlig og individuelt tilpasset helsehjelp. Samtidig er personopplysninger om helseforhold og sosiale omstendigheter blant de mest private og sensitive, og det er derfor viktig at disse er godt beskyttet både rettslig og i praksis. I Personvernkommisjonens mandat pekes det nettopp på at helsesektoren er ett av flere områder der personvernutfordringene er mange og vanskelige. Pasientene må gi fra seg opplysninger om sykdom, uførhet, livsstil og andre personlige forhold av betydning for behandlingen for å nyte godt av slik helsehjelp. Hvis legen ikke har tilstrekkelige opplysninger om pasientens sykdomsbilde, forhistorie og situasjon ellers, vil behandlingen kunne lide, og pasienten kan i verste fall risikere å få gal behandling. Det er derfor et grunnleggende hensyn, og i pasientens interesse, at behandlende helsepersonell faktisk har tilgang til nødvendig informasjon om den pasienten de behandler. Mens få vil bestride dette, er det på den annen side flere kritiske røster som påpeker at «helsetjenesten lekker» og at det er en stadig videre personkrets som med rette eller urette får tilgang til sensitiv informasjon om pasienter. Det er særlig dette som aktualiserer personvernspørsmål i helsetjenesten og som vil være tema i denne delen av rapporten.

Begrepet personvern refererer i vid forstand til tiltak hvis formål er å beskytte individets autonomi (selvbestemmelse) og personlige integritet (se avsnitt 4.2.3). I helsetjenesten omfatter dette vern av så vel fysisk som psykisk integritet, og viser seg særlig i form av kravet om informert samtykke til helsehjelp og rett til vern mot spredning av personlige opplysninger (se pasientrettighetsloven § 4-1, § 3-2, § 3-6 og helsepersonelloven kapittel 5). I denne delen av rapporten er det personvern i betydningen vern mot spredning av personlige opplysninger som er i fokus.

Helseforskning er et annet viktig tema når man diskuterer bruk av opplysninger om helseforhold, enten forskningen skjer innenfor eller utenfor selve helsetjenesten. Pasientjournalen er en av de viktigste kildene for medisinsk forskning, noe som medfører at brytningen mellom behovet for å skjerme individet på den ene siden og samfunnets behov for å utvikle ny kunnskap og bedre behandlingsmetoder på den andre, aktualiseres.

Helseforskningsloven ble vedtatt 20.6.2008 og er omtalt i rapportens avsnitt 7.2.3. Personvernkommisjonen har observert at deler av lovforslaget har vært gjenstand for kritikk og diskusjon fra høringsinstansene og fagmiljøet. Dette gjelder blant annet bruken av såkalte brede samtykker, det vil si samtykker som omfatter ett eller flere overordnede forskningsformål og forskningsfelt, uten at de enkelte detaljer som ønskes forsket på er spesifisert. Personvernkommisjonen har merket seg at et mindretall i helse- og omsorgskomiteen har ytret bekymring for om et slikt samtykke vil være i samsvar med internasjonale konvensjoner om personvern. En annen del av kritikken mot loven gjelder svekkelse av personvernet ved at mulighetene for avidentifisering ikke utnyttes fullt ut. Etter Personvernkommisjonens oppfatning kan en tilsvarende kritikk også rettes mot andre sentrale helseregistre, som for eksempel Norsk pasientregister, hvor lovgiver i nyere tid har vist en tendens til å velge bort pseudonymisering som personvernfremmende tiltak.

På grunn av tidshensyn har Personvernkommisjonen dessverre måttet avgrense mot personvernutfordringer som kan oppstå når helseopplysninger brukes i medisinsk og helsefaglig forskning. Se imidlertid kommentarene i avsnitt 16.5.6 om registre og de mange gode formål.

16.1 Utviklingstrekk

Helsetjenesten skal løse mange oppgaver i tilknytning til forebygging, diagnostikk og behandling av sykdom og skade. Bruk, lagring og kommunikasjon av helseopplysninger er en nødvendig forutsetning for å kunne gi helsehjelp, og derfor et karakteristisk trekk ved den moderne helsetjeneste. Ikke bare helsehjelp, men også andre velferdstilbud, forutsetter behandling av helseopplysninger, for eksempel beslutninger om trygd, sosialhjelp og arbeidsrettede tiltak. Fordi helse- og sosialtjenestens oppgaver har vært jevnt ekspanderende de siste årtier, samtidig som ressursene ikke er ubegrenset, har også kravet om kostnadseffektivitet blitt viktig. Det er et viktig formål å utforme tilbud som gir mest mulig helse-effekt for pengene, både på individ- og samfunnsnivå.

Typisk for vår tid er at man imøtekommer kravet om kostnadseffektivitet ved å samle inn og bruke data, gjerne gjenbruk av opplysninger som allerede er samlet inn i den løpende virksomheten. Disse dataene brukes som indikatorer på produksjon og produktivitet. Et problem i personvernsammenheng er når slik gjenbruk av data resulterer i at sensitive pasientopplysninger tilflyter administrasjonen/virksomheten på alle nivå. Jo flere som får tilgang til opplysninger, desto vanskeligere er det å sikre mot lekkasjer til uvedkommende.

Et annet karakteristisk trekk ved den moderne velferdsstaten er økt samarbeid mellom ulike velferdsetater. Dette kommer også til uttrykk i lovgivningen, som i økende grad har åpnet opp for samarbeid mellom ulike velferdsetater og for utveksling av personopplysninger på tvers av etatene. Dette reiser viktige personvernspørsmål (se nærmere drøfting om NAV-reformen i avsnitt 16.5.5). Det forventes i mange tilfeller at helsepersonell samarbeider med andre fagfolk for å kunne gi et helhetlig og koordinert tilbud til grupper med behov for langvarig og sammensatt hjelp. Dette kan gi pasientene bedre behandling og oppfølgning, men «prisen» er at flere får kunnskap om intime forhold vedrørende pasienten. Samarbeid på tvers av instanser og disipliner er blitt et honnørord for dagens velferdsstat, men det er viktig å påpeke at medaljen har en bakside, og da særlig i relasjon til personvern.

Et annet aspekt ved moderne velferdstilbud er kravet om selvbestemmelse og medvirkning. Pasientrettighetsloven slår fast hovedregelen om informert samtykke som forutsetning for helsehjelp (§ 4-1), og samtykke fra pasienten er også det viktigste rettsgrunnlag for å videreformidle opplysninger om pasienten (jf. pasientrettighetsloven § 3-6, 2. ledd og helsepersonelloven § 22). Pasientrettighetsloven § 3-1 gir pasienten rett til å medvirke ved gjennomføring av helsehjelpen, og herunder medvirke ved valg mellom tilgjengelige og forsvarlige undersøkelses- og behandlingsmetoder. Prinsippet om medvirkning kommer også til uttrykk i annen lovgivning, se eksempelvis arbeids- og velferdsforvaltningsloven § 6, som pålegger arbeids- og velferdsdirektoratet å sørge for at representanter for brukerne får mulighet til å uttale seg i forbindelse med planlegging, gjennomføring og evaluering av etatens tjenester. Her er det altså ikke brukeren selv, men representanter for brukerne, som skal høres. Samme lov inneholder imidlertid i en bestemmelse som sier at tjenestetilbudet så langt som mulig skal utformes i samarbeid med brukeren (§ 15, 2. ledd). Kravet om brukermedvirkning er begrunnet i hensynet til å styrke pasientens eller klientens verdighet og autonomi, og er også med på å styrke ulike tiltaks eller inngreps legitimitet i befolkningen.

I moderne tid er det ikke minst innføringen av datateknologi som har endret og effektivisert helsevesenet og bidratt til et økende press i retning av å samle inn og registrere opplysninger og gjøre dem tilgjengelige for flere formål (forskning, statistikk, kvalitetssikring, behandling, planlegging, styring, etc.). Sammenstilling av registre kan gi kunnskap om viktige sammenhenger, for eksempel mellom fødselsvekt og forekomst av sykdom, og mellom røyke- og kostholdsvaner og kreftutvikling. Data innhentet for ett formål kan være nyttige også for andre formål. Dette har ført til stor etterspørsel etter data samlet inn i helsetjenesten, ikke minst fra forskningsmiljøer. Fokuset på positive sider ved å registrere helseopplysninger kan imidlertid overskygge og hindre den nødvendige oppmerksomhet rundt viktige personvernspørsmål.

Parallelt med tendensen til økt informasjonsflyt, både internt i helsetjenesten og mellom instanser, øker naturligvis behovet for og kravet om trygghet: Helseopplysninger oppfattes som sensitive, og må reguleres og behandles i overensstem-

melse med dette. Visshet om at sensitiv informasjon håndteres forsvarlig, ikke videreformidles til uvedkommende og ikke misbrukes, er avgjørende for befolkningens tillit til helsevesenet. I denne sammenheng oppstår spørsmålet om hvem som er «uvedkommende» og hva som er «misbruk». Om dette vil det kunne herske ulike oppfatninger, avhengig av hvilket ståsted og hvilke erfaringer man har.

I tillegg til de mange lovfestede unntakene fra taushetsplikten (se nedenfor i 16.4.3), har innføring av elektronisk databehandling, herunder elektroniske pasientjournaler, medført at det er blitt enklere å skaffe seg tilgang på informasjon om pasienter, også for personer som ikke deltar i behandlingen av pasienten. Man trenger ikke lenger å lete i arkiver og papirjournaler, men kan ved hjelp av tastetrykk på en datamaskin enkelt finne fram til informasjon om bestemte pasienter. Selv om helsepersonell generelt sett er bevisst på sin taushetsplikt, viser enkeltsaker at det noen ganger handles feil og at det mange steder kommuniseres om taushetsbelagte opplysninger i strid med bestemmelsene om taushetsplikt. Dette kan skyldes både manglende kunnskap om taushetspliktens innhold og omfang, ukultur eller ubetenksomhet, og det er ikke alltid lett å si sikkert hva som er årsaken til at taushetsplikten krenkes (Helsetilsynet 2005). Ren nysgjerrighet kan nok også spille inn som motiv i enkelte tilfeller (se omtale av saken I mot Finland i avsnitt 16.4.1 nedenfor). I et brev til Helse- og omsorgsdepartementet fra 2007 viser Datatilsynet til flere henvendelser som gjelder uautoriserte oppslag/innsyn i pasientjournaler («snoking») (Datatilsynet 2007b).

Mange av unntaksbestemmelsene fra hovedregelen om taushetsplikt er vage og skjønnspregede, og kan nok by på visse problemer i praksis. Dette kan ha betydning for overholdelsen av gjeldende bestemmelser om taushetsplikt. Personvernkommisjonen antar likevel at et større problem er manglende bevissthet omkring og kompetanse i forhold til sikring av helseopplysninger, ikke minst i forbindelse med elektroniske kommunikasjonsformer. Et eksempel på dette er en pasient som opplevde at opplysninger om bruk av medisin ble offentliggjort på Internett ved at et brev fra fastlege til Fylkesmann var søkbart i Fylkesmannens postliste (Aftenposten.no 2008a). Datatilsynets direktør uttalte i den anledning at tilsynet ukentlig mottar henvendelser om sensitive opplysninger som legges ut på Internett, og at det generelt sett er en manglende årvåkenhet i forhold til behandling av personopplysninger ved elektronisk kommunikasjon (ibid.). Dette medfører utilsiktede krenkelser av taushetsplikten, som altså ikke skyldes mangler ved regelverket, men manglende etterlevelse av regelverket på grunn av manglende årvåkenhet og sviktende rutiner.

16.2 Grunnleggende hensyn og spenningsforholdet mellom dem

Hensynet til ivaretakelse av helseformål er et overordnet hensyn i helsetjenesten. Statens oppgave er å bevilge penger og organisere helsetjenesten slik at borgernes behov for helsehjelp ivaretas på en tilfredsstillende måte. Til tross for at hensynet til helse er viktig, er ikke ressursene ubegrenset og samfunnet må foreta økonomiske prioriteringer og vurderinger knyttet til kostnadseffektivitet. Dette kommer blant annet til uttrykk i pasientrettighetsloven § 2-1, 2. ledd om rett til nødvendig helsehjelp fra spesialisthelsetjenesten. Det fremgår her at retten bare gjelder dersom pasienten kan ha forventet nytte av helsehjelpen og kostnadene står i rimelig forhold til tiltakets effekt.

Helsetjenestens ivaretakelse av helseformål og økonomi må skje innenfor de rammer som følger av lovgivning, menneskerettighetskonvensjoner, etc. Helse er i seg selv en menneskerettighet, jf. Konvensjonen om økonomiske, sosiale og kulturelle rettigheter artikkel 12, og forutsetter at tjenestetilbudet må holde en forsvarlig og adekvat standard i lys av statens tilgjengelige ressurser og utviklingsnivå. Videre er respekt for privatliv en grunnleggende menneskerettighet som må ivaretas av helsetjenesten i overensstemmelse med artikkel 8 i Den europeiske menneskerettighetskonvensjon og artikkel 17 i Konvensjonen om sivile og politiske rettigheter. Pasientens privatliv er beskyttet blant annet gjennom bestemmelser om helsepersonells taushetsplikt, som fra gammelt av har vært bærebjelken i lege-pasient-forholdet og som er en viktig forutsetning og grunnorm for helsetjenesten. Uten tillit til behandleres taushetsplikt ville mange unnlate å oppsøke helsehjelp når de trenger det. Det er alminnelig akseptert at taushetsplikten er avgjørende for det tillitsforholdet som må herske mellom pasient og helsetjeneste. Pasienten skal kunne betro seg til sin behandler i trygg forvissning om at informasjonen ikke bringes videre, og behandler skal kunne motta opplysninger med visshet om at disse ikke kan kreves utlevert (Helsetilsynet 2005). Se nærmere om helsepersonells taushetsplikt i Rasmus-

sen (1997), og Kjønstad (2007, ss. 271-313). Ikke bare leger, men alt helsepersonell, og alt samarbeidende personell, herunder de som bistår med elektronisk bearbeiding av opplysninger, eller som bistår med service og vedlikehold av utstyr, har taushetsplikt, i den grad ingen av unntakene fra taushetsplikten kommer til anvendelse.

Det er særlig to grunnleggende hensyn som må avveies i helsesektoren: Hensynet til en best mulig helsetjeneste på individ- og samfunnsnivå, med tanke på både kvalitet og effektivitet, på den ene siden, og hensynet til tradisjonelle rettssikkerhetsgarantier, herunder personvern, på den andre. Pasientrettighetslovens formålsbestemmelse (§ 1-1) gir uttrykk for disse hensyn:

> «Lovens formål er å bidra til å sikre befolkningen lik tilgang på helsehjelp av god kvalitet ved å gi pasienter rettigheter overfor helsetjenesten. Lovens bestemmelser skal bidra til å fremme tillitsforholdet mellom pasient og helsetjeneste og ivareta respekten for den enkelte pasients liv, integritet og menneskeverd.»

Loven gir her uttrykk for de tungtveiende hensyn som gjør seg gjeldende på helsetjenestens område: På den ene siden hensynet til å sikre befolkningen helsetjenester av god kvalitet, og på den andre siden hensynet til å opprettholde tillit og ivareta respekten for pasientens liv, integritet og menneskeverd. I relasjon til de spørsmål som tas opp i denne innstillingen, ivaretakelse av personvern, er det særlig hensynet til overordnede helseformål som må veies opp mot hensynet til den enkeltes integritet og menneskeverd. Begrepet menneskeverd skal her forstås i humanistisk tradisjon, inspirert av Kants lære om at individet aldri må behandles som et middel alene, men samtidig som et mål i seg selv (Barbosa da Silva 2006).

Formålsbestemmelsen til helseregisterloven gir mer direkte uttrykk for at personvern er viktig når den sier at formålet med loven «er å bidra til å gi helsetjenesten og helseforvaltningen informasjon og kunnskap *uten å krenke personvernet*, slik at helsehjelp kan gis på en forsvarlig og effektiv måte» (uthevet her). Formålsbestemmelsen fremhever videre forskning og statistikk som viktige redskaper, ved at «informasjon og kunnskap om befolkningens helseforhold, årsaker til nedsatt helse og utvikling av sykdom» skal tas i bruk av hensyn til administrasjon, kvalitetssikring, planlegging og styring. Det presiseres at loven skal sikre at helseopplysninger blir behandlet i samsvar med «grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på helseopplysninger» (§ 1).

Denne bestemmelsen fanger opp spenningsfeltet mellom ulike interesser og behov, samt den store utfordring samfunnet står overfor med tanke på både å ivareta enkeltmenneskets interesser og gjennom kvalitetssikring, forskning, styring, etc., å styrke helsetjenestens kunnskapsgrunnlag og sørge for en oppdatert og effektiv helsetjeneste. Formålsbestemmelsen gir likevel et tydelig signal om at personvernhensyn bør veie tungt på vektskålen når ulike hensyn avveies.

16.3 Pasientjournalen og IKT-utviklingen

Pasientjournalen står sentralt i den personvernproblematikk som berører helsevesenet. En pasientjournal kan defineres som et arbeidsverktøy for helsepersonell, der alle medisinske forhold av betydning for pasientens helse dokumenteres, så som hvilke observasjoner og vurderinger som er gjort og hvilke tiltak som er satt i verk. Slike pasientjournaler har vært i bruk i Norge siden 1800-tallet. De papirbaserte pasientjournalene har i den nyere tid antatt helt andre dimensjoner enn tidligere. En journal ved Akershus universitetssykehus er eksempelvis gjennomsnittlig på 120 sider, og én sykehusseng gir opphav til tolv nye journaler pr. år (sykehuset har nesten 500 senger). Til tross før økende bruk av mikrofilm, krever journalmaterialet stor plass, samtidig som tilgjengeligheten til materialet ikke alltid er like god. Informasjonen fremstår ofte som spredt og man er plaget av mye «dobbeltarbeid» (Brøten 2000).

Helsepersonelloven slår fast at pasientjournaler kan føres elektronisk, (jf. § 46, 1. ledd, se også helseregisterloven § 6), noe som gjøres i økende grad. De fleste private og offentlige sykehus og helsetjenester baserer seg nå på elektronisk journalføring. Norges teknisk naturvitenskapelige universitet (NTNU) fikk i 2003 i oppdrag å etablere et kompetansemiljø for elektronisk pasientjournal, finansiert av Norges Forskningsråd, noe som har bidratt til utvikling og kompetanseoppbygging, ikke minst gjennom etablering av Norsk senter for elektronisk pasientjournal (NSEP), som er et tverrfaglig forskningsmiljø ved NTNU. Kompetansesenter for IKT i helse- og sosialsektoren AS (KITH) ble etablert i 1999 (opprinnelig het det Kompetansesenter for informasjonsteknologi i helsevesenet) for å bidra til en koordinert IT-utvikling i helse- og sosialsektoren. Senteret er et

aksjeselskap eid av Helse- og omsorgsdepartementet (70 %), Arbeids- og inkluderingsdepartementet (10, 5 %) og Kommunenes Sentralforbund (19,5 %). Disse fagmiljøene ønsker å bidra til utvikling av kunnskapsbasert og koordinert bruk av elektronisk pasientjournal, noe de har fått et klart mandat til fra myndighetene.

Bruken av elektronisk pasientjournal reiser spørsmål om hva slags informasjon som kan og skal lagres, hvem som skal ha tilgang, hvordan bestemmelsene om taushetsplikt skal overholdes, hvordan informasjon skal bevares gjennom skifte av teknologi etc. Det foreligger et stort behov for standardisering og samordning av helsetjenestens informasjons- og kommunikasjonssystemer. Sosial- og helsedirektoratet anbefaler i rundskriv IS-1/2002 en standard utviklet av KITH (Nystadnes 2005).

Den raske utviklingen innen informasjons- og kommunikasjonsteknologi (IKT) har ført til at informasjon kan frambringes og spres hurtigere enn før, er raskere tilgjengelig og kan finnes med større treffsikkerhet. IKT har også økt mulighetene for at informasjon hele tiden er oppdatert (uten at dette alltid er tilfelle i praksis). De tekniske systemene muliggjør bedre tilgangskontroll (kontroll av hvem som frembringer bestemte opplysninger om enkeltpersoner), og det kan føres logg (oversikt, elektronisk sporing) over hvem som har innhentet informasjon. Informasjonssikkerheten, dvs. kvaliteten på den informasjonen som lagres, kan også bedres ved hjelp av IKT, for eksempel ved mulighetene for systematisk oppdatering. Mulighetene for kryptering bidrar til at informasjonen kan sikres bedre mot innsyn fra utenforstående.

På den annen side har utviklingen innen IKT noen klare ulemper sett fra et personvernperspektiv, ikke minst på helsevesenets område.

Det lagres store samlinger av sensitive opplysninger, som flere rent faktisk har tilgang til, dersom det ikke implementeres organisatoriske og tekniske rutiner som hindrer økt tilgang. Mens man tidligere måtte ha fysisk tilgang til pasientjournalen, enten ved å oppsøke arkivet eller ved at den fantes tilgjengelig på et legekontor eller en sengepost, er denne nå bare et par tastetrykk unna. Det er særlig dette som utfordrer taushetsplikten. Det er blitt lettere å få tilgang til, og derved kunne misbruke, informasjon. Det er særlig informasjonens tilgjengelighet som gir større potensial for misbruk.

Personvernkommisjonen har videre observert at de systemene og den programvare som i dag er i bruk i helsetjenesten ikke alltid anvendes slik at taushetsplikten ivaretas på en tilfredsstillende måte. Her er det nødvendig med personvernfremmende tiltak på flere plan: Ikke bare lovgivning og holdningsskapende tiltak må til, men også tiltak for å fremme ledelsesansvar, og uvikling av og opplæring i programvare som fremmer personopplysningsvern. Mulighetene for tekniske og menneskelige feil må begrenses og IKT-bruken må tilpasses helsetjenestens krav, ikke minst ivareta bestemmelsene om taushetsplikt og behovet for effektiv tilgangskontroll.

16.4 Rettigheter, plikter og rettslig regulering

16.4.1 Retten til privatliv

Den grunnleggende rettighet som står på spill ved uberettiget kommunikasjon av helseopplysninger er retten til privatliv. Det følger av Den europeiske menneskerettskonvensjon (EMK) artikkel 8 (1) at enhver har rett til respekt for sitt privatliv. Etter vedtakelsen av menneskerettsloven skal EMK gjelde som norsk lov og ved motstrid gå foran bestemmelser i annen lovgivning (se § 3 jf. § 2 nr. 1). Retten til privatliv er dermed en grunnleggende menneskerett som må respekteres i alle sammenhenger. Denne rettigheten har stor aktualitet i helsesektoren, idet helseopplysninger, for eksempel om sykdom, behandling og helseplager, utvilsomt tilhører den enkeltes private sfære, som er omfattet av det menneskerettslige vern om privatlivet. Dette slås utvetydig fast i en fersk dom fra Den europeiske menneskerettsdomstol (EMD) – I mot Finland (dom av 17. juli 2008) – der en HIV-positiv sykepleier hevdet at sykehusets datasystem ikke beskyttet henne mot uautorisert innsyn i hennes pasientdata fra andre ansatte ved sykehuset. Domstolen peker på at statens forpliktelse ikke er begrenset til en «negativ» plikt til selv å avstå fra privatlivskrenkelser, men også en «positiv» forpliktelse til å iverksette effektive tiltak for å verne om borgernes privatliv (ibid., avsnitt 36). Denne sikringsplikten omfatter også vern mot krenkelser av tredjemenn som ikke handler på vegne av det offentlige (Jacobs og White 2006, s. 243), for eksempel privat ansatt helsepersonell.

For helsetjenesten innebærer dette en plikt til å sørge for et effektivt vern om pasienters privatliv i form av et system som gir sikker beskyttelse mot uberettiget innsyn i og flyt av helseopplysninger (I mot Finland, avsnittene 35-37). Det presise-

res i den nevnte dommen at det ikke er tilstrekkelig at lovgivningen garanterer beskyttelse mot uautorisert innsyn i data, så lenge det ikke etableres tilfredsstillende systemer og rutiner som i praksis gir et effektivt vern om den enkeltes privatliv. Det er heller ikke tilstrekkelig å etablere klageordninger med muligheter for kompensasjon for skader forårsaket av ulovlig innsyn. I dommen sies det: «What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place» (avsnitt 47). Finland ble dømt for brudd på EMK artikkel 8 (1), med den begrunnelse at de nødvendige sikkerhetstiltak for å beskytte den enkeltes privatliv ikke var etablert.

Dommen er en viktig påminnelse om at retten til privatliv og beskyttelse av private opplysninger i helsevesenet i stor grad handler om praktiske og effektive tiltak for å hindre urettmessig tilgang til informasjon om andre. Dette krever ikke bare lovregulering, men etablering av praktiske løsninger som gir den nødvendige beskyttelse i praksis. Det er derfor nødvendig å stille to spørsmål i forhold til beskyttelse av personopplysninger på helsevesenets område: Er den eksisterende rettslige regulering tilstrekkelig? Er reguleringen gjennomført på en måte som faktisk sikrer et effektivt vern om privatlivet til den enkelte?

I det følgende gjennomgås deler av den nasjonale lovgivningen som beskytter den enkeltes privatliv på helsevesenets område.

16.4.2 Krav til behandling av personopplysninger og helseopplysninger

Det er flere lover som er sentrale for behandling av personopplysninger i helsevesenet. Generelt vil behandling av helseopplysninger i helsetjenesten og helseforvaltningen reguleres av helseregisterloven, som suppleres av personopplysningsloven på viktige punkter. Hovedtrekkene i disse lovene er omhandlet foran, i kapittel 7, og det vises i hovedsak til denne fremstillingen. Her vil vi fremheve noen punkter som er særlige relevante for dette kapittelet. I tillegg til disse lovene finnes det spesialbestemmelser hva gjelder registrering og bruk av opplysninger i pasientjournal, i blant annet helsepersonelloven, pasientrettighetsloven, samt regler for håndtering av biologisk materiale i biobankloven.

Helseregisterloven har særlige regler for opprettelsen av behandlingsrettede helseregistre, herunder journalsystemer. Plikten til å føre journal følger av helsepersonelloven § 39. Pasientjournalen er altså en lovhjemlet behandling som ikke trenger konsesjon fra Datatilsynet og som heller ikke er betinget av pasientens samtykke. Helsepersonelloven § 40 gir bestemmelser om journalens innhold. Journalen skal føres i samsvar med god yrkesskikk og skal inneholde relevante og nødvendige opplysninger om pasienten og helsehjelpen, samt de opplysninger som er nødvendige for å oppfylle meldeplikt eller opplysningsplikt fastsatt i lov eller i medhold av lov. Journalen skal være lett å forstå for annet kvalifisert helsepersonell, og det skal fremgå hvem som har ført opplysningene i journalen.

Helseregisterloven hjemler også opprettelsen av andre lokale, regionale og sentrale helseregistre i helsetjenesten og helseforvaltningen.

Når det gjelder annen behandling av personopplysninger i helsetjenesten, må disse følge reglene i helseregisterloven § 5, som forutsetter at behandlingen er i samsvar med personopplysningsloven.

Personopplysningslovens utgangspunkt er at personopplysninger bare kan behandles dersom den registrerte har samtykket, behandlingen er lovhjemlet, eller behandlingen er nødvendig for ulike formål, herunder for «å utføre en oppgave av allmenn interesse», eller for «å ivareta den registrertes vitale interesser», se lovens § 8. Når det gjelder behandling av sensitive opplysninger, herunder helseopplysninger, gjelder det tilleggsvilkår som nevnt i § 9, herunder at «behandlingen er nødvendig for å beskytte en persons vitale interesser, og den registrerte ikke er i stand til å samtykke» (bokstav c) og «behandlingen er nødvendig for forebyggende sykdomsbehandling, medisinsk diagnose, sykepleie eller pasientbehandling eller for forvaltning av helsetjenester, og opplysningene behandles av helsepersonell med taushetsplikt» (bokstav g). Behandling av sensitive personopplysninger, herunder helseopplysninger, skal som hovedregel ha konsesjon fra Datatilsynet, jf. personopplysningsloven § 33.

Helseregisterloven § 16 pålegger den databehandlingsansvarlige (den som bestemmer formålet med behandlingen og hvilke hjelpemidler som skal brukes, jf. § 2 nr 8[1]) og databehandleren (den som behandler personopplysninger på vegne av den behandlingsansvarlige, jf. § 2 nr 9) gjennom planlagte og systematiske tiltak å sørge for «tilfredsstillende informasjonssikkerhet med hen-

[1] Dette vil typisk være direktøren ved sykehus og andre helseinstitusjoner.

syn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger». Personopplysningslovens sikkerhetsbestemmelser gjelder tilsvarende, jf. helseregisterloven § 36 og personopplysningsforskriftens kapittel 2.

Videre skal den databehandlingsansvarlige etablere og vedlikeholde de tiltakene som er nødvendige for å oppfylle lovens krav (internkontroll, jf. § 17). Dette er viktige bestemmelser med tanke på å sikre helseopplysningers konfidensialitet i praksis, ikke minst med tanke på etablering av datasystemer og saksbehandlingsrutiner som ivaretar de nødvendige kravene. Kravet om tilfredsstillende informasjonssikkerhet må i relasjon til helseopplysninger innebære rettslige, tekniske og praktiske løsninger som medfører at bestemmelser om taushetsplikt for helsepersonell og andre yrkesgrupper faktisk etterleves.

16.4.3 Helsepersonells og andre yrkesgruppers taushetsplikt

Til tross for at helsepersonells taushetsplikt er et grunnprinsipp i helsesektoren, gjøres det mange unntak fra taushetsplikten (se nærmere nedenfor i avsnitt 16.4.3.5). Strømmen av helseopplysninger som med lovgivers tillatelse går til ulike faglige og administrative instanser er stor og økende. Mange av de opplysningene som meldes til helsemyndigheter og andre tjener utvilsomt gode formål. Helsepersonell har eksempelvis meldeplikt til ulike etater og instanser, og videre har de plikt til å delta i kontroll- og tilsynsarbeid for å øke kvaliteten i helsetjenesten. Helsepersonell kan for eksempel ikke med henvisning til taushetsplikt unnlate å melde fra om fødsler, dødsfall og betydelig personskade (se helsepersonelloven §§ 35, 36 og 38), og de kan ikke unnlate å gi opplysninger til Statens helsetilsyn og Helsetilsynet i fylket som må anses påkrevd for utøvelsen av tilsyn med helsepersonellets virksomhet (helsepersonelloven § 30). Dette omfatter også opplysninger om enkeltpersoner. Den som yter helsehjelp har videre rett til å gi opplysninger til virksomhetens ledelse når dette er nødvendig for å kunne gi helsehjelp, eller for internkontroll og kvalitetssikring av egen virksomhet. I slike tilfeller skal imidlertid individualiserende kjennetegn i for eksempel pasientjournaler utelates så langt som mulig (jf. helsepersonelloven § 26, 1. ledd), ved «sladding» av navn, utelatelse av irrelevant informasjon, etc. På dette punktet kan det være grunn til å undersøke om regelverket følges i praksis.

En viktig dimensjon i relasjon til unntak fra helsepersonells taushetsplikt er at det er mange utenforstående aktører – ikke minst innenfor arbeids- og velferdsforvaltningen (arbeidskontor, trygdekontor, sosialkontor) – som av ulike grunner har stor interesse av helsetjenestens nedtegnelser om pasienter. Et sentralt hensyn i denne sammenheng er kontroll; samfunnets behov for å føre tilsyn med og kontrollere at velferdstilbudene anvendes etter sin hensikt (hindre misbruk). Personvernkommisjonen antar at dette generelt sett er et legitimt formål all den tid Norge på mange områder har sjenerøse velferdstilbud som vil kunne misbrukes. Men behovet for kontroll kan likevel ikke rettferdiggjøre at det iverksettes tiltak som ikke er formåls- eller forholdsmessige i det enkelte tilfelle. Det er derfor nødvendig med årvåkenhet slik at kontrollfunksjonen utøves på en måte som er forenlig med grunnleggende rettssikkerhetsgarantier og respekt for den enkelte.

I det følgende gis en kort gjennomgang av regelverket om taushetsplikt med påfølgende betraktninger om de utfordringene man står overfor i dagens helsetjeneste.

16.4.3.1 Hvem har taushetsplikt?

Helsepersonell skal etter helsepersonelloven § 21 «hindre at andre får adgang eller kjennskap til opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold som de får vite om i egenskap av å være helsepersonell». Bestemmelsen omfatter alt helsepersonell, enten de utfører arbeid for offentlig eller privat helsetjeneste- eller institusjon.[2] Tilsvarende bestemmelse om taushetsplikt for «personlige forhold» finner vi i forvaltningsloven § 13, 1. ledd, som gjelder for enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, herunder administrativt ansatte som arbeider ved offentlige helseinstitusjoner.

Hva gjelder administrativt ansatte i privat helsetjeneste (sekretærer, kontoransatte), vil disse normalt måtte underskrive taushetserklæring som vilkår for ansettelse, og deres taushetsplikt følger da av det avtalerettslige forholdet mellom arbeidstaker og arbeidsgiver. Arbeidsgiver – en privatpraktiserende lege eller en privat helseinstitusjon – vil i slike tilfeller være databehandlingsansvarlig med et selvstendig ansvar for å implementere rutiner som ivaretar pasientenes konfidensialitet, se helseregisterloven § 17. Det følger videre av helse-

[2] Hvem som er helsepersonell følger av helsepersonelloven § 3, og omfatter personell med autorisasjon etter § 48 eller lisens etter § 49, personell i helsetjenesten eller i apotek som utfører helsehjelp og elever og studenter som i forbindelse med helsefaglig opplæring utfører helsehjelp.

registerloven § 15, som gjelder for både offentlig og privat virksomhet (se § 3, 2. ledd), at enhver som behandler helseopplysninger i medhold av loven har taushetsplikt etter forvaltningsloven §§ 13 til 13e og helsepersonelloven. Databehandler er enhver som behandler helseopplysninger på vegne av den databehandlingsansvarlige, jf. lovens § 2 nr 9. Dette må forstås slik at også administrativt ansatte i privat helsetjeneste som behandler helseopplysninger omfattes av taushetsplikt etter helseregisterloven.

Helseregisterloven § 13 bestemmer videre at bare den databehandlingsansvarlige, databehandlere og den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet, kan gis tilgang til helseopplysninger. Tilgang kan bare gis i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt. Dette innebærer i praksis at arbeidsgiveren har ansvar for at bare personell med et berettiget arbeidsrelatert behov gis tilgang til helseopplysninger eller andre opplysninger om pasienter, og at dette skjer i overensstemmelse med «gjeldende bestemmelser» om taushetsplikt, herunder bestemmelsen i helseregisterloven § 15.

16.4.3.2 Taushetspliktens innhold

Helsepersonelloven § 21 pålegger helsepersonell å «hindre» at andre får adgang eller kjennskap til opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold som de får vite om i egenskap av å være helsepersonell. Dette innebærer noe forenklet at plikten omfatter alle personlige opplysninger om en pasient som vedkommende helsepersonell mottar i forbindelse med sin yrkesutøvelse (om helse, familie, sosiale relasjoner, arbeid, rusproblemer, etc.), også om opplysningene mottas etter arbeidstid. Det avgjørende er at opplysningene mottas fordi man er lege, sykepleier etc.

Personvernkommisjonen vil peke på at det mange steder eksisterer uheldige rutiner med hensyn til ivaretakelse av taushetsplikt, for eksempel ved at legen kommuniserer med pasienten i påhør av andre pasienter og annet helsepersonell. Dette forekommer særlig der pasienten ikke har enerom, men ligger på rom med flere, der sengene er atskilt med forheng som ikke hindrer at andre hører det som blir sagt. Det kan ikke antas at pasienten stilltiende samtykker til at sensitive opplysninger på denne måten deles med andre, og det er derfor nødvendig med nye rutiner for å sikre forsvarlig håndheving av taushetsplikten. Den tradisjonelle «legevisitten» respekterer ikke pasientens personvern og er utgått på dato.

Taushetsplikten gjelder ikke bare en plikt til å tie, men også en generell plikt til å verne opplysninger mot uvedkommendes innsyn. Følsomme opplysninger i pasientjournaler, notater, korrespondanse etc. skal ikke på noen måte være tilgjengelige for uvedkommende. Helsetilsynet har i enkeltsaker konkludert med at det ikke er akseptabelt at pasientjournaler som skal makuleres pakkes i plastsekker og kastes på søppeldyngen, eller at gamle datamaskiner kastes uten at lagrede opplysninger i tilstrekkelig grad er fjernet (det samme vil følge av sikkerhetsbestemmelsene i personopplysningsforskriften). Det er heller ikke akseptabelt at helsepersonell i forbindelse med flytting av en praksis ikke har kontroll med hvem som flytter pasientarkivet, hvor dette blir plassert og om alt er blitt flyttet (Helsetilsynet 2005). Pasientinformasjon må håndteres og oppbevares på forsvarlig vis. Helsetilsynet har eksempelvis konstatert brudd på taushetspliktreglene i en sak der en lege flyttet sin praksis og etterlot pasientopplysninger usikret i de gamle lokalene. I en annen sak fant Helsetilsynet at det forelå brudd på taushetsplikten da pasientjournaler lå åpent på gulvet i et ulåst kontorområde (ibid).

16.4.3.3 I forhold til hvem gjelder taushetsplikten?

Helsepersonelloven § 21 innebærer at helseopplysninger og andre personlige opplysninger som helsepersonell får vite om en pasient i kraft av sin stilling eller sitt yrke er taushetsbelagte. Plikten er formulert slik at helsepersonellet «skal hindre at andre får adgang eller kjennskap» til disse. Ordet «andre» må tolkes strengt og omfatter i utgangspunktet alle andre enn helsearbeideren selv. Dette er imidlertid mer et ideelt utgangspunkt enn en praktisk realitet, ettersom lovgivningen selv åpner for en rekke unntak fra taushetsplikten. Dette er en erkjennelse av at de sterke hensynene som begrunner taushetsplikten noen ganger må vike for andre viktige hensyn; hensynet til pasienten selv, viktige samfunnsmessige interesser og hensynet til andre.

Det følger av helsepersonelloven § 25, 1. ledd at taushetsbelagte opplysninger kan gis til samarbeidende personell «når dette er nødvendig for å kunne gi forsvarlig helsehjelp». Informasjon kan altså ikke utveksles i større utstrekning enn det som er nødvendig for at forsvarlig helsehjelp skal kunne gis. Statens helsetilsyn påpeker at en del

helsearbeidere tror at de fritt kan utveksle pasientopplysninger seg i mellom, ettersom de alle har taushetsplikt (ibid.). Dette er imidlertid en misforståelse av reglene om taushetsplikt, ettersom det avgjørende er at utvekslingen må være påkrevet for å kunne yte forsvarlig helsehjelp. Helsetilsynet finner videre grunn til å informere om at det heller ikke er slik at personell som gjennom sitt arbeid har tilgang til pasientjournaler har fullmakt til å lese alle pasientjournaler (ibid.). Det er den opplysningene gjelder som har rådighet over opplysningene. Dette kommer til uttrykk i helsepersonelloven § 25, som presiserer at opplysninger kun kan gis til samarbeidende personell i den grad pasienten ikke motsetter seg dette. Lovens ordlyd viser her klart at det er pasienten som skal styre hvem som får tilgang til taushetsbelagte opplysninger om ham eller henne, og at pasienten også kan styre hvor mye informasjon som kan formidles videre. Bestemmelsen forutsetter at pasienten kan nekte informasjonsutveksling, selv om dette er nødvendig for forsvarlig helsehjelp. Pasienten kan for eksempel kreve at en bestemt prøve ikke analyseres ved det lokale sykehus, men sendes utenbys. Det foreligger imidlertid ikke uten videre noen informasjonsplikt for helsepersonell før slik informasjonsutveksling skjer. Dette innebærer at det er pasienten som må gi uttrykkelig beskjed dersom hun eller han ikke ønsker at samarbeidende personell skal få bestemte opplysninger som normalt vil formidles i forbindelse med behandlingen. Hensynet til personvern kan imidlertid tilsi at pasienten i enkelte tilfeller bør informeres før informasjon utveksles, med adgang til å motsette seg dette. Dette kan være aktuelt når det dreier seg om særskilt sensitiv informasjon eller hvor det er tvilsomt av andre grunner om pasienten ville gitt samtykke til informasjonsutveksling (jf. Befring og Ohnstad 2001, note 73).

Helsepersonell og helsetjeneste har som utgangspunkt og hovedregel taushetsplikt i forhold til andre etater. Dette innebærer at informasjon fra fastlegen for eksempel ikke kan sendes til sosial- eller trygdekontoret, med mindre pasienten samtykker til dette. Det heter i helsepersonelloven § 32, 1. ledd at den som yter helsehjelp i sitt arbeid skal «være oppmerksom på forhold som bør føre til tiltak fra sosialtjenestens side, og skal av eget tiltak gi sosialtjenesten opplysninger om slike forhold etter å ha innhentet samtykke fra pasienten, eller så langt opplysningene ellers kan gis uten hinder av taushetsplikt etter § 21». Hovedregelen er dermed at det gjelder et krav om samtykke for å formidle opplysninger videre, i tråd med helsepersonelloven § 22, 1. ledd og pasientrettighetsloven § 3-6, 2. ledd, som begge slår fast at taushetsplikt faller bort i den utstrekning pasienten samtykker. Unntak gjelder dersom det foreligger lovhjemmel for å gi opplysninger videre, for eksempel til NAV.

Loven oppstiller ikke bestemte formkrav til samtykket. Kravet om samtykke er imidlertid et krav om pasientens tillatelse. I forbindelse med informasjonsbehandling vil dette som regel medføre krav om en uttrykkelig og informert tillatelse fra pasienten for å sikre frivillighet, oversikt over konsekvenser og moden overveielse (ibid., note 59). Det er en forutsetning for gyldig samtykke at pasienten er i stand til å treffe en slik beslutning, med andre ord et krav om samtykkekompetanse, jf. pasientrettighetsloven § 4-3. Samtykket trenger likevel ikke være skriftlig, og i noen tilfeller vil også et indirekte eller underforstått (stilltiende) samtykke kunne godtas (ibid.), se nærmere i det følgende.

Helsetilsynet har lagt til grunn at i situasjoner der det er behov for mye samarbeid og hyppig utveksling av informasjon om en pasient mellom ulike helseinstitusjoner, helsepersonell eller andre instanser, kan kravet om uttrykkelig samtykke i forkant av hver utveksling av informasjon gjøre at effektiv behandling vanskeliggjøres. Det har derfor oppstått en praksis der såkalt «implisitt samtykke» godtas, i betydningen at pasienten antas å godta utlevering av vedkommendes taushetsbelagte opplysninger (Helsetilsynet 2005). Dette er i overensstemmelse med anerkjennelsen av såkalt «stilltiende samtykke», som i pasientrettighetsloven § 4-2 sidestilles med uttrykkelig samtykke. Stilltiende samtykke foreligger dersom det ut fra pasientens handlemåte og omstendighetene for øvrig er sannsynlig at hun eller han godtar helsehjelpen, jf. pasientrettighetsloven § 4-2, 1. ledd annen setning. Til tross for den formelle likestillingen i lovteksten, må imidlertid kravene til samtykke øke med inngrepets alvorlighetsgrad, slik at stilltiende samtykke til helsehjelp i praksis kun er aktuelt ved mer ordinære eller rutinepregede behandlingsformer. Når det gjelder kommunikasjon av helseopplysninger basert på implisitt, underforstått eller stilltiende samtykke, er dette bare akseptabelt i den grad forutsetningen om at pasienten aksepterer dette utvilsomt kan legges til grunn. Hvis det åpenbart (utvilsomt) er i pasientens interesse, men vedkommende av en eller annen grunn ikke er i stand til å gi samtykke, vil stilltiende samtykke kunne godtas. I tillegg vil helsepersonelloven § 7 om plikt til å yte helsehjelp i

øyeblikkelig hjelp-situasjoner, selv om pasienten motsetter seg helsehjelpen, medføre både rett og plikt til å innhente og videreformidle de helseopplysninger som den medisinske behandling av pasienten nødvendiggjør. Utover dette må det ses hen til opplysningenes art, situasjonen for øvrig og vedkommendes antatte vilje. Dersom det hersker tvil om hva som er pasientens vilje, utgjør ikke stilltiende samtykke et tilstrekkelig grunnlag for å utlevere helseopplysninger.

16.4.3.4 Uautorisert tilgang til taushetsbelagte helseopplysninger

De største utfordringer og problemer i relasjon til kommunikasjon av og tilgang til helseopplysninger er etter Personvernkommisjonens oppfatning knyttet til uautorisert tilgang til helseopplysninger internt i helsetjenesten, samt at et økende antall samarbeidsinstanser får lovhjemlet tilgang til helseopplysninger om enkeltpersoner. Dette utfordrer taushetsplikten og sentrale personverninteresser som konfidensialitet og kontroll over egne opplysninger.

Ikke minst har problemet knyttet til uautorisert tilgang sammenheng med innføring av elektronisk pasientjournal, som har gjort det enklere for ansatte i helsetjenesten å få tilgang til pasientopplysninger. Datatilsynet peker på at overgangen fra papir til elektroniske pasientjournaler (EPJ) har medført en økning i personvernrisikoen i helsesektoren og at problematikken særlig er knyttet til at «mer informasjon er lettere tilgjengelig for flere, lettere å spre til uvedkommende (Internett) og i den grad opplysningene først er spredd, er det vanskeligere å begrense skaden for pasientene som er rammet» (Datatilsynet 2007b).

Datatilsynet hevder videre at det er vanskelig å angi et kvalifisert omfang av uautoriserte oppslag i pasientjournaler, men at kombinasjonen av «en liberal holdning når rettigheter til systemer skal tildeles, mangelfulle funksjoner for å begrense tilgang og få reelle kontrollmekanismer, kan skape grobunn for misbruk» (ibid.). Det pekes på at denne form for misbruk av tillit kan gjøre stor skade for de personene som rammes og svekke helsetjenestens posisjon i samfunnet. Det vises til en MMI-undersøkelse, gjengitt i Dagbladet den 5. juni 2005, der det anslås at 86 prosent av de ansatte i helsevesenet bekrefter at det er utbredt å se i pasientjournalene ut over det som er nødvendig (ibid.).

Dette var bakgrunnen for at Datatilsynet foreslo lovfesting av pasientens rett til innsyn i journalloggene i pasientrettighetsloven. Selv om tilsvarende rett også kan utledes av retten til innsyn etter bestemmelser i personopplysningsloven og helseregisterloven, mente Datatilsynet at det her var viktig å synliggjøre retten til innsyn i journalloggen for pasienten ved å nedfelle den i pasientrettighetsloven, på linje med retten til innsyn i pasientjournalen. Formålet med forslaget var å gi pasienten bedre kontroll over hvem som åpner journalen av ren nysgjerrighet. Departementet har fulgt opp forslaget i forslag til forskrift om informasjonssikkerhet og elektronisk tilgang til helseopplysninger i behandlingsrettede helseregistre (se http://www.regjeringen.no/nb/dep/hod/dok/hoeringer/hoeringsdok/2008/horing--tilgang-til-behandlingsrettede-.html?id=533748) . Forslaget er på høring i skrivende stund, med høringsfrist 12. januar 2009.

Det er imidlertid vedtatt bestemmelser som retter seg mot selve «snokingen». En ny bestemmelse i helsepersonelloven § 21a (tilføyd ved lov 9. mai 2008 nr. 34) slår fast at det er forbudt å «lese, søke etter eller på annen måte tilegne seg, bruke eller besitte opplysninger som nevnt i § 21 uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift». Dette er en viktig bestemmelse i lys av erfaringene med uberettiget «snoking» i pasientjournaler som har medført en tiltakende mistillit til helsetjenestens evne til å ivareta personvernet. Forbudet kan i så måte være med på å styrke det tillitsforholdet som må herske mellom legen og pasienten og mellom befolkningen og helsetjenesten. Tilsvarende bestemmelse er tilføyd i helseregisterloven, i en ny § 13a. Også denne bestemmelsen er viktig fra et personvernperspektiv, fordi den gir et klart rettslig signal om at det er ulovlig å tilegne seg helseopplysninger om andre når dette ikke er begrunnet i legitime, helserelaterte formål.

Personvernkommisjonen kommer nærmere inn på tilgang til taushetsbelagt informasjon internt i og på tvers av foretak nedenfor.

16.4.3.5 De mange unntakene fra taushetsplikten

Taushetsplikten er ikke lenger så absolutt som den var før. En rekke unntak følger av lovgivningen, og medfører en ganske vidtgående begrensning av taushetsplikten. Asbjørn Kjønstad fremhever at alle de lovbestemte innskrenkninger i taushetsplikten uthuler grunnprinsippet om taushetsplikt (Kjønstad 2007 s. 311-312). Han viser til at det foreligger ca. 50 bestemmelser som

pålegger helsepersonell plikt til å gi meldinger av ulike slag eller som gir adgang til å meddele ellers taushetsbelagte opplysninger. Selv om hvert enkelt av disse unntak i og for seg er godt begrunnet og ivaretar legitime formål, kan selve omfanget av unntak fra taushetsplikten bidra til en uthuling av grunnprinsippet om taushetsplikt (ibid. s. 312).

Unntakene fra taushetsplikten kan grupperes i 1) unntak som gjelder bruk av opplysninger internt i den enkelte helseinstitusjon, 2) unntak som gjelder utlevering av opplysninger av hensyn til pasienten og den helsehjelpen som skal gis, 3) unntak som gjelder utlevering av opplysninger til eksterne tilsyns- og kontrollorganer, 4) unntak som gjelder utlevering av opplysninger til sentrale helseregistre, og 5) unntak som gjelder utlevering av opplysninger til andre utenforstående (pårørende, forskere, politi, media). Personvernkommisjonen har ikke kapasitet til å gå gjennom alle de lovbestemte unntakene fra taushetsplikten, men vil anbefale en systematisk gjennomgang for å motvirke en uheldig uthuling og sikre at det bare gjøres unntak der det utvilsomt er til beste for pasienten eller er åpenbart nødvendig av hensyn til andre personer eller viktige samfunnsinteresser.

16.5 Personvernkommisjonens observasjoner

Personvernkommisjonen har lyttet til mange aktører i sin bestrebelse på å få oversikt over utfordringene for personvernet i helsevesenet, både behandlere, brukere, forskere, administratorer og andre med særlig kompetanse og innsikt. Formålet med informasjonsinnhentingen har vært å bidra til en så bred og nyansert debatt som mulig, for å få viktige problemstillinger fram i lyset.

Den 19. mai 2008 arrangerte kommisjonen et åpent møte om personvern i helsesektoren, der det særlig ble satt fokus på elektronisk pasientjournal fra henholdsvis et behandlings- og pasientperspektiv, og på tekniske muligheter knyttet til slik journalføring. Videre ble problemstillinger knyttet til samarbeid og informasjonsutveksling tatt opp, med fokus på den såkalte NAV-reformen. Spørsmål knyttet til økt registrering av helseopplysninger ble belyst gjennom innlegg om IPLOS, der både myndighetene og representanter for pasientene ble hørt. Møtet ble avsluttet med en paneldebatt om personvern og helsedata med fokus på rettslige og praktiske løsninger. Det kom fram mye viktig informasjon på det åpne møtet som Personvernkommisjonen har hatt god nytte av i sitt videre arbeid. Nedenfor vil vi fremheve noen særlig viktige observasjoner.

16.5.1 Elektronisk pasientjournal – EPJ

Helsepersonell har plikt til å journalføre den helsehjelpen de gir. Dette medfører at pasientene ikke kan motta helsehjelp uten at personopplysninger blir registrert i en journal, jf. helsepersonelloven § 39 og journalforskriften § 5. En journal er en sammenstilling av opplysninger om en enkelt pasient. Pasientene har ingen mulighet til å velge om det skal føres journal; dersom man ønsker helsehjelp, må man akseptere at opplysninger blir nedtegnet skriftlig i journalen. Årsaken til dette er at journalen også har til formål å dokumentere den behandlingen som er gitt og det arbeidet helsepersonellet har gjort. Slik dokumentasjon kan også pasienten få nytte av, for eksempel ved senere behov for å se egen sykehistorie eller for å dokumentere eventuell feilbehandling.

Pasientjournaler er etter dagens ordning etablert på virksomhetsnivå, det vil si at virksomheter som yter helsehjelp er forpliktet til å opprette et pasientjournalsystem. Plikten til å dokumentere den helsehjelpen som er gitt påhviler imidlertid også det enkelte helsepersonell. Systemet må opprettes slik at det er mulig å etterleve krav fastsatt i lov eller i medhold av lov, herunder taushetsplikten. Pasientjournalene kan være papirbaserte eller elektroniske, men det er den elektroniske pasientjournalen, EPJ, som er tema i det følgende.

16.5.1.1 Journaltilgang internt i virksomheter

Bestemmelsene om taushetsplikt setter som nevnt skranker for hvem som skal ha tilgang til opplysninger i pasientjournalen. Selv om det finnes flere unntak, er den klare hovedregelen at bare de som skal yte helsehjelp skal ha tilgang til og innsyn i journalen. Skranker for tilgang internt i virksomheten følger også av helseregisterloven § 13, som stiller krav om at tilgang bare skal gis i den grad det er «nødvendig for vedkommendes arbeid». Tilsvarende kan også utledes av sikkerhetsbestemmelsen i helseregisterloven § 16 og kravet om at virksomheten skal iverksette tiltak som sikrer opplysningenes konfidensialitet.

I mai 2006 gjennomførte Helsetilsynet i Hordaland og Datatilsynet et felles tilsyn ved Helse Bergen. Tilsynet avdekket blant annet at de elektroniske pasientjournalene ikke var forsvarlig vernet mot innsyn fra ansatte som ikke har legitimt

behov for opplysningene. Både i forkant og etterkant av dette har Datatilsynet gjennomført flere kontroller overfor helseforetak hvor det har blitt avdekket svært vide tilgangsrettigheter for ansatte i virksomheten. I et brev fra Helsetilsynet til Helse- og omsorgsdepartementet fra mars 2008 (Helsetilsynets ref. 2008/578) uttales det at «mangelfull tilgangsstyring til elektroniske pasientjournaler truer taushetsplikten i sykehus».

Ett av hovedprinsippene i den såkalte EPJ-standarden er følgende:

> «Ingen skal gis tilgang til flere journalopplysninger enn det som er nødvendig for å kunne gjennomføre de oppgaver som følger av den rolle vedkommende har. Når behovet for tilgang til journalopplysninger opphører, for eksempel fordi et besluttet tiltak er ferdig gjennomført, skal tilgangen til journalopplysningene opphøre.»

Det foreligger i dag flere systemer for elektroniske pasientjournaler, men det er foreløpig ingen felles pasientjournal for alle pasienter (dette vil bli omtalt nærmere nedenfor). Noen av journalsystemene ivaretar tilgangskontroll på den måten at det er behandlende helsepersonell ved den enheten pasienten er til behandling som har tilgang til den elektroniske journalen. De enkelte virksomhetene kan imidlertid selv styre varighet og hvem som har tilgang til pasientjournalene ved den enkelte sengepost eller poliklinikk. Det er eksempler på at det i forhold til planlagte innleggelser er rutiner for at det åpnes for journaltilgang for det helsepersonellet som har oppgaver i forbindelse med behandlingen av pasienten en uke før innleggelse, og at tilgangen opphører 14 dager etter utskrivelsen. Dette betyr at epikrise (sammendrag av journalen fra sykehusoppholdet) og eventuelle prøvesvar må foreligge innen 14 dager. Slike prosedyrer vil innebære en klar styrking av personvernet for pasientene og bidra til økt tillit hos de pasientene som har opplevd mangelen på tilgangskontroll som et problem. Dersom disse prosedyrene etterleves, vil det kun være de som har behov for innsyn for å kunne yte helsehjelp som gis tilgang til og dermed innsyn i pasientjournalen. Dette innebærer en klar forbedring i forhold til tidligere, hvor alle ansatte som har vært utstyrt med journaltilgang har hatt tilgang til alle pasientjournaler til enhver tid, uten noen form for begrensninger.

Det kan være flere årsaker til at regelverket om taushetsplikt og personvern ikke etterleves i praksis, herunder manglende kunnskaper og skolering om personvern, mangelfulle tekniske systemer, dårlige rutiner, liten respekt for regelverket, svak ledelse og manglende prioritering av personvern. Uansett årsak mener Personvernkommisjonen at det er nødvendig å sette fokus på praktiseringen av tilgang til pasientopplysninger, herunder de tekniske løsningene som benyttes. Sett fra et personvernståsted er det avgjørende at tilgangsstyringen innrettes etter pasientenes behov for diskresjon, og ikke etter helsepersonells ønske om informasjon. Det er fullt mulig samtidig å sikre journaltilgangen som er nødvendig for å gi pasienter forsvarlig helsehjelp. Det kreves her vilje til å iverksette de tiltakene som må til for å gjennomføre gjeldende regelverk, noe som forutsetter en bevisstgjøring i mange ledd og på alle nivåer i helsetjenesten. Personvernkommisjonen er kjent med at det nå arbeides aktivt med disse problemstillingene i mange helseforetak.

16.5.1.2 Om aktivitetslogger og gjennomgangen av disse

Det følger av sikkerhetsbestemmelsene i personopplysningsforskriften kapittel 2 at både autorisert og forsøk på uautorisert bruk av informasjonssystemet skal registreres, se forskriften § 2-8 og 2-16. Disse loggene skal lagres i minst 3 måneder, jf. § 2-16. Dersom en virksomhet opererer med vid tilgang begrunnet et helsefaglig behov, må dette følges opp med systematisk gjennomgang av loggen. Loggen vil være et viktig hjelpemiddel når virksomheten skal avdekke om ansatte gjør oppslag i pasientjournalen uten å være autorisert for det, eller uten at et tilstrekkelig saklig behov foreligger, og er følgelig et viktig teknisk tiltak for å avdekke brudd på taushetsplikten.

Personvernkommisjonen har observert at tilsyn overfor helseforetak har avdekket få kontrollressurser og svake kontrollrutiner, noe som medfører at risikoen for å bli avslørt dersom man gjør oppslag i en journal uten at det foreligger et tjenstlig behov er liten. Det er ofte slik at loggen gjennomgås når kjente personer eller sykehusansatte har vært pasienter, ellers ikke. Denne praksisen er kjent for de ansatte, og loggføringen må dermed antas å ha liten preventiv effekt. Det er etter Personvernkommisjonens mening uheldig dersom eksisterende virkemidler for å avdekke snoking i journalen ikke utnyttes.

Det finnes flere eksempler på saker hvor pasienter har kontaktet pasientombudet og anmodet om bistand til å få undersøkt hvem som har utøvd innsyn i deres journal. Bakgrunnen for en slik

henvendelse har for eksempel vært at private opplysninger er gjort kjent for uvedkommende. Når pasienten ikke selv har formidlet de aktuelle opplysninger til noen, må kommunikasjon av opplysningene enten skyldes brudd på taushetsplikten eller at noen som ikke har vært involvert i behandlingen har vært inne og lest i journalen. En gjennomgang av loggen i disse tilfellene har avdekket «snoking» med påfølgende sanksjoner mot «snokeren», noe som bidrar til å styrke pasientenes rettssikkerhet. Det var tidligere et problem at man ikke kunne konstatere lovbrudd dersom «snokeren» ikke også hadde overtrådt taushetsplikten. Dette er nå avhjulpet ved vedtakelsen av den tidligere omtalte § 21a i helsepersonelloven.

Personvernkommisjonen er videre kjent med at pasienter som har bedt om innsyn i tilgangsloggen til sin elektroniske journal, har mottatt en logg som har vært lite opplysende. Det har vært nødvendig med møter eller videre korrespondanse for å avklare nærmere hva tilgangsloggen egentlig viser. Det bør derfor settes krav til at tilgangsloggen på en enkel måte viser hvem som har lest i journalen, og hva den enkelte eventuelt har nedtegnet.

16.5.1.3 Journaltilgang på tvers av virksomheter

Økt samhandling på tvers av helseforetak har skapt et behov for bredere og raskere tilgang til relevant og nødvendig informasjon om pasienten. Dagens regelverk setter imidlertid skranker for når slik informasjonsutveksling kan skje. Det følger av helseregisterloven § 13 at kun den databehandlingsansvarlige (og andre som jobber i virksomheten) kan gis tilgang til helseopplysninger. Tilgangen skal dessuten være i samsvar med taushetsplikten. Taushetspliktsbestemmelsene fordrer som tidligere nevnt at det som hovedregel innhentes samtykke fra pasienten før journalopplysninger utleveres.

Dersom det foreligger saklig behov og pasientens samtykke innhentes, vil det i konkrete tilfeller være lovlig for helsepersonell å be om innsyn i journalen ved et annet sykehus. Rent praktisk kan slikt innsyn ordnes ved at det sykehuset som sitter med relevant informasjon utleverer etter konkret forespørsel, eller at den som ber om informasjon selv autoriseres for å gjøre oppslag. Inntil det er utviklet en tilfredsstillende nasjonal infrastruktur med tilgangsstyring og tilhørende loggføring av aktiviteter og identiteter på tvers av virksomheter, er det imidlertid ikke uproblematisk for et helseforetak å «åpne» journalsystemet sitt for direkte tilgang for en annen virksomhet, da slik ad hoc «åpning» gjerne er forholdsvis uoversiktlig mht. hvem som får tilgang. Ofte er systemene heller ikke tilrettelagt for at man skal kunne avgrense tilgangen til hva som skal anses som relevant informasjon i det aktuelle tilfellet. Krav om tilgang etter konkret forespørsel vil for øvrig kunne skape merarbeid hos det foretaket som anmodes om å utlevere opplysningene, og ikke nødvendigvis bidra til raskere informasjonsoverføring enn dagens praksis hvor anonymiserte journaldokumenter overføres pr. telefaks. Et annet problem er at det ikke alltid er mulig å innhente pasientens samtykke til utlevering av helseopplysninger, for eksempel i akuttsituasjoner.

I 2007 fikk Sosial- og helsedirektoratet i oppdrag fra Helse- og omsorgsdepartementet å utrede tiltak for enklere tilgang til elektroniske pasientjournaler og vurdere behovet for lovendringer. Direktoratet avga sin rapport i mars 2008 (Sosial- og helsedirektoratet 2008). Det kommer i denne utredningen klart fram at det fra spesialisthelsetjenestens side ønskes en åpen fullmakt slik at sykehus og andre virksomheter kan avtale seg imellom at direkte tilgang skal iverksettes. Direktoratet mener imidlertid at det er vanskelig å se at tiden er moden for å gi slike fullmakter, all den tid man internt har mangelfull tilgangstyring, med den følge at taushetsplikten i sykehus brytes. Anbefalingen fra direktoratet er altså at man skynder seg langsomt i forhold til å åpne for direkte tilgang på tvers av virksomheter. Direktoratet konkluderer med at nye og mer omfattende endringer i ansvaret for å ha og bruke pasientopplysninger bør gjøres først etter at det har vært foretatt en offentlig utredning som gir mulighet for grundig vurdering av de mange spørsmålene som melder seg i denne forbindelse.

Da Personvernkommisjonen var i sluttfasen av sitt arbeid, sendte Helse- og omsorgsdepartementet ut et forslag om å lovhjemle tilgang på tvers av virksomheter på høring (http://www.regjeringen.no/nb/dep/hod/dok/hoeringer/hoeringsdok/2008/horing--tilgang-til-behandlingsrettede-.html?id=533748). Her forslås det to løsninger som har til formål å imøtekomme helsetjenestens behov for informasjon på tvers av virksomhetsgrenser; tilgang til eksisterende virksomhetsinterne behandlingsrettede helseregistre på tvers av virksomheters grenser og etablering av virksomhetsovergripende behandlingsrettede helseregistre. Forslaget har høringsfrist i januar 2009. Personvernkommisjonen har ikke hatt anledning til å

sette seg inn i forslaget, men vil likevel knytte noen generelle kommentarer til spørsmålet om tilgang på tvers av virksomheter.

Personvernkommisjonen ser at behovet for samhandling og effektivisering av helsetjenesten på tvers av foretak og virksomheter på sikt bør imøtekommes. Det er viktig, også av hensyn til pasienten, at relevante opplysninger er tilgjengelige ved behov. Dette gjelder ikke minst i situasjoner der liv og helse står på spill. Personvernkommisjonen antar at rene personvernhensyn normalt vil måtte vike dersom en pasients liv og helse er truet og kan reddes, dersom det gis innsyn i vedkommendes journal. Avveiningen er imidlertid ikke like enkel i tilfeller der behovet for opplysningene ikke er fullt så påtrengende. Her vil helsefaglige behov i større grad måtte avveies mot andre viktige hensyn, ikke minst hensynet til å ivareta pasientens personvern.

Det er ikke tvil om at økt tilgang til pasientjournalen utfordrer pasientens interesse i integritet og konfidensialitet. En ivaretakelse av de ulike hensynene forutsetter at det iverksettes tiltak som imøtekommer behovet for å ha nok opplysninger når det er nødvendig, samtidig som det ikke gis tilgang til flere opplysninger enn det som er relevant. Før det åpnes for journaltilgang på tvers av virksomheter, må det foretas en grundig avveining av både fordeler og potensielle ulemper. En del av pasientene som benytter seg av retten til fritt sykehusvalg og fornyet vurdering, gjør dette nettopp for å kunne starte med blanke ark. Disse pasientene vil ofte være opptatt av at journalopplysninger fra tidligere behandlingssted ikke skal følge dem videre til andre behandlere.

Ekstern tilgang til pasientjournalen i en virksomhet forutsetter etter Personvernkommisjonens oppfatning god styring og kontroll internt. Med tanke på de svakhetene som både Datatilsynet og Helsetilsynet har avdekket gjennom sine tilsyn når det gjelder tilgangskontroll internt, bør man som Sosial- og helsedirektoratet påpeker, gå forsiktig fram med tanke på å utvide tilgangen til også å omfatte eksterne parter. Dersom en utenforstående virksomhet skal gis direkte tilgang til sykehusets journaler, vil den ansvarlige virksomheten i prinsippet miste noe av kontrollen med overholdelse av taushetsplikten. Som Personvernkommisjonen har fremhevet ovenfor, innebærer taushetsplikten også en aktiv plikt til å hindre at uvedkommende får tilgang til taushetsbelagt informasjon. Av hensyn til pasientens interesse i å ha kontroll over egne opplysninger bør utlevering til utenforstående i størst mulig grad baseres på et gyldig samtykke fra pasienten. Uthuling av samtykkekravet i denne sammenheng bør bare aksepteres i den grad det er påtrengende nødvendig for å kunne yte forsvarlig helsehjelp, for eksempel i en akuttsituasjon hvor det ikke er tid eller anledning til å innhente samtykke.

Etter Personvernkommisjonens oppfatning fordrer økt tilgjengelighet til pasientjournalen at pasienter kan ha tillit til at det ikke er verken juridisk, teknisk eller faktisk mulig for utenforstående å tilegne seg informasjon man ikke skal ha. Dette forutsetter kontinuerlig og systematisk opplæring og oppdatering av helsepersonells kunnskaper om gjeldende regelverk om taushetsplikt og personvern. I tillegg kreves holdningsskapende arbeid hos både helsepersonell og sykehusledelse, samt fortsatt strenge regler for når det kan gjøres unntak fra taushetsplikten og hovedregelen om samtykke til slikt unntak.

16.5.2 Bør pasienten få tilgang til egne journalopplysninger i elektronisk format?

På Personvernkommisjonens åpne møte om personvern innen helsesektoren ble følgende spørsmål stilt til panelet: «Når får pasienten journalen sin på en minnepinne?»

I motsetning til papirjournaler, som både opptar plass og som kan leses av alle som har fysisk tilgang til dem, kan minnepinner og smartkort utstyres med tilgangskoder som sikrer at kun den som kjenner tilgangskoden og som har fysisk adgang til mediet, får tilgang.

Dersom pasienter hadde tilbud om å få utlevert en kryptert minnepinne eller smartkort som inneholdt alle journalnedtegnelser fra deres kontakter med helsetjenesten, kunne dette gi pasienter tilgang på egne journalopplysninger på et kompakt og fleksibelt elektronisk format. For å få tilgang, måtte pasienten koble minnepinnen til en USB-port på egen PC, eller lese av smartkort i en dertil egnet kortleser, koblet til sin egen PC. Pasienten ville kunne bringe minnepinnen med seg til lege og sykehus for å sikre at all nødvendig informasjon er tilgjengelig for behandlende helsepersonell, noe som vil ha klare helsefaglige fordeler i situasjoner der den aktuelle virksomheten ikke selv har alle nødvendige opplysninger om pasienten.

Personvernkommisjonen vil understreke at utlevering av journal på minnepinne eller smartkort ikke er et hensiktsmessig alternativ til en nasjonal elektronisk pasientjournal (EPJ) for å sikre for-

svarlig helsehjelp i akutt-situasjoner og lignende. Det er flere grunner til dette:

1. Pasienter vil miste minnepinner og smartkort. En viss andel av slike vil også gå i stykker, enten pga. uvøren behandling, eller som følge av fabrikasjonsfeil. Det vil derfor være urimelig å pålegge borgere å bære en slik minnepinne eller smartkort på seg til enhver tid. Man kan altså ikke basere arkivering og/eller transport av kritiske heleopplysninger på denne typen elektronisk medium. Minnepinnen eller smartkortet kan kun benyttes som et tilbud om en portabel og sikker elektronisk kopi av journalen som et alternativ til å få utlevert en papirkopi av journalen for pasienter som ønsker en elektronisk kopi.
2. For å kunne gi forsvarlig behandling i alle situasjoner, må behandlende helsepersonell ha tilgang til opplysninger i pasientens journal. Dette forutsetter at journalføringsplikten, slik som i dag, ligger hos den virksomheten som behandler pasienten. Minnepinner vil derfor bare kunne være en tilleggssikkerhet for pasienter som innlegges ved andre sykehus hvor de ikke er kjent fra før, og hvor minnepinnen inneholder opplysninger av vital betydning for behandling av pasienten.

Personvernkommisjonen vil samtidig understreke at et slikt elektronisk tilbud forutsetter at det etableres en tilfredsstillende infrastruktur for standardformater, metadata, kryptering, administrasjon av tilgangskoder og programvare for visning og utskrift av krypterte data på pasientenes PC-er. Denne må både ivareta tilfredsstillende informasjonssikkerhet og gjøre sikker bruk av lagringsmediet og tilhørende programvare for den som kjenner tilgangskoden like enkelt og transparent som å bla i en papirutskrift. Det er åpenbart urealistisk å gå ut fra at pasientene selv skal beherske eller forholde seg til nødvendig teknologi for kryptering, etc. Å etablere en slik infrastruktur vil derfor kreve en betydelig og målrettet innsats. Personvernkommisjonen antar at dette vil kunne være mulig å få til på sikt, men at det fremdeles er langt fram før man er kommet så langt.

16.5.3 Personvern og praktisering av offentlighet

Det er et faktum at ikke alle brukere av helsetjenesten er fornøyd med den behandlingen de har mottatt, og av den grunn ønsker å fremme en klage. Saksgangen er som regel at det sendes en skriftlig klage til Helsetilsynet i fylket, direkte fra klager selv eller via et pasientombud.

Helsetilsynet er et forvaltningsorgan, og dermed underlagt offentlighetslovens bestemmelser. Dette medfører at organets dokumenter som hovedregel er offentlige, og at media eller andre kan be om innsyn (jf. offentlighetsloven § 2). Prinsippet om offentlighet er en viktig del av vårt demokrati og kan bidra til at det rettes søkelys mot kritikkverdige forhold i samfunnet. Taushetsbelagte opplysninger skal imidlertid unntas offentlighet, jf. offentlighetsloven § 5a og forvaltningsloven § 13.

Innkomne brev registreres i Helsetilsynets postlister, og media har adgang til å be om innsyn i disse. Det er vanlig at journalister ber om innsyn i saksdokumentene i slike klagesaker for å se om dette er noe som bør omtales i pressen. I disse tilfellene skal Helsetilsynet foreta en vurdering av om det kan gis innsyn i enkelte deler av dokumentet uten at taushetsplikten krenkes, for eksempel ved at direkte identifiserbare opplysninger sladdes. Regelen er at dokumentet for øvrig «er offentlig» så sant de frigitte delene ikke «alene gir et åpenbart misvisende bilde av innholdet eller de unntatte opplysninger utgjør den vesentligste del av dokumentets innhold», jf. offentlighetsloven § 5a, 2. ledd. Dersom innsyn gis, er det dermed avgjørende at alle opplysninger som kan bidra til gjenkjennelse av klager fjernes. Dette gjøres dessverre ikke alltid, og det finnes flere eksempler på at pasienter som følge av dette har blitt ufrivillig omtalt i mediene.

Årsaken til manglende anonymisering kan enten skyldes mangelfulle rutiner hos virksomhetene eller menneskelige feil. Slike feil vil i mange tilfeller oppleves som svært krenkende for den pasienten det gjelder, da opplysninger om helseforhold, som vi har tidligere omtalt, er noe man i stor grad ønsker å holde for seg selv. Konsekvensen av at det skjer feil på dette området kan i verste fall føre til at folk unnlater å klage, noe som igjen undergraver de hensynene offentlighetsloven er ment å ivareta. Fra flere pasientombud får kommisjonen opplyst at pasienter nettopp vegrer seg for å klage til for eksempel Helsetilsynet fordi de frykter medieomtale. Dette er bekymringsfullt, og kan føre til at tilsynsmyndighetene ikke mottar tilbakemeldinger de trenger for å gjennomføre sine kontrolloppgaver. Det foreligger også eksempler på at klager, etter å ha fått kjennskap til at det er praktisert dokumentinnsyn, direkte har anmodet journalisten om ikke å omtale saken av frykt for å bli gjenkjent, uten at dette har blitt tatt tilføl-

ge. Dette oppleves som et ytterligere overgrep for den det gjelder.

Et beslektet problem knytter seg til vansker med å ivareta anonymitet. Det er ikke alltid godt nok at navn på klager fjernes, det kan være nødvendig å fjerne opplysninger om kjønn, diagnose, type behandling, eller hvilken kommune det gjelder, for å hindre at klageren gjenkjennes i små lokalsamfunn.

Det er viktig for samfunnet at kritikkverdige forhold i helsevesenet blir offentlig kjent. Men pasienten det gjelder har krav på å få sin identitet vernet. Dersom man sørger for å ivareta reglene om anonymitet, vil dette imøtekomme både samfunnets behov for å føre kontroll med helsevesenet og pasientenes personvern.

16.5.4 Personvern og kontroll

Personvernet kan også være utsatt i forhold til intern og ekstern kontroll av helsetjenesten. Flere tilsynsmyndigheter, som Riksrevisjonen, NAV og Helsetilsynet, har hjemmel til å innhente fullstendige journaler for sine tilsyns- og kontrolloppgaver, mens det i forhold til interne kontroller gis et forbehold i helsepersonelloven § 26 om at «opplysningene skal så langt det er mulig, gis uten individualiserende kjennetegn».

Det kan stilles spørsmål ved begrunnelsen for at eksterne tilsynsmyndighetene ikke omfattes av den samme begrensningen om at opplysningene så langt det er mulig skal gis uten individualiserende kjennetegn. Den enkelte pasient har som følge av dette ingen kontroll med at de opplysninger han eller hun har gitt i største fortrolighet til helsepersonell ikke blir kjent av andre som pasienten absolutt ikke ønsker skal ha denne kunnskapen.

Som eksempel kan det vises til at Riksrevisjonen innhenter et stort antall journaler fra spesialisthelsetjenesten og kobler disse mot journaler fra kommunehelsetjenesten i sin kontrollvirksomhet. Det bør problematiseres om ikke kontrolloppgavene kan utføres uten identifiserende kjennetegn. Journalene kunne for eksempel vært avidentifisert og blitt utstyrt med en form for kode (avidentifisering/pseudonymisering), og revisjonen kunne vært gjennomført uten at de aktuelle pasientene ble utsatt for personvernkrenkelser. Det er viktig ut fra minimalitetsprinsippet at man foretar en kritisk vurdering både av hvilke opplysninger det er nødvendig å gi tilgang til for å oppfylle kontrollbehovet og i hvilken grad det er nødvendig at disse er personidentifiserbare. Det stilles spørsmål ved om hensynet til personvernet ble tilstrekkelig utredet i forbindelse med vedtakelsen av de ulike kontrollhjemlene

Også internt i helsetjenesten syndes det mot kravet i helsepersonelloven § 26 om at opplysningene så langt det er mulig skal gis uten individualiserende kjennetegn. Det er velkjent at enkelte virksomheter ikke ser hensiktsmessigheten av anonymisering og argumenterer med økt arbeidsmengde og at opplysningene ville bli spredt til like mange dersom journalene skulle blitt gjenstand for en anonymiseringsprosess i forkant av kontrollen. Personvernkommisjonen vil fremheve at lovens krav om at individualiserende kjennetegn så langt som mulig skal utelates er strengt og må respekteres.

16.5.5 Samarbeid og informasjonsutveksling. Særlig om NAV-reformen

Et kjennetegn ved den moderne velferdsstaten er at det tilbys tjenester basert på kunnskap fra en rekke fagfelt. Medisin, helsefag, psykologi, sosialfag og barnevern er sentrale områder av betydning for borgernes helse og velferd, og de administreres av henholdsvis helsetjenesten, sosialetaten og barnevernet. Det er en økende erkjennelse av at ulike etater i stor grad bør samarbeide for å sikre borgerne et faglig godt og helhetlig tilbud. Dette kommer nå til uttrykk i ulike lovbestemmelser, for eksempel bestemmelsene om rett til individuell plan for pasienter eller brukere med behov for langvarige og koordinerte helsetjenester, se eksempelvis pasientrettighetsloven § 2-5, loven om psykisk helsevern § 4-1 og arbeids- og velferdsforvaltningsloven § 15, 3. ledd. Disse planene forutsetter i stor grad at det etableres samarbeid mellom ulike etater om behandling og oppfølging av pasienten eller klienten.

I 2006 ble arbeids- og velferdsforvaltningsloven (NAV-loven) vedtatt, som er det rettslige grunnlaget for sammenslåingen av arbeids- og trygdeetaten til den nye Arbeids- og velferdsetaten (NAV). Dette omtales gjerne som NAV-reformen; Norges største offentlige reform i nyere tid. Den nye «etaten», som skal betraktes som ett organ i forhold til taushetsplikt (se nedenfor), består av arbeids- og velferdsetaten og deler av kommunens tjenester, jf. NAV-loven § 2. Formålet med loven er «å legge til rette for en effektiv arbeids- og velferdsforvaltning, tilpasset den enkeltes og arbeidslivets behov og basert på en helhetlig og samordnet anvendelse av arbeidsmarkedsloven,

folketrygdloven, sosialtjenesteloven og andre lover som forvaltes av arbeids- og velferdsforvaltningen», jf. lovens § 1. Å få flere i arbeid, tilbud om individuelt tilpassede tjenester og å hindre «kasteballer» i systemet er viktige formål i denne sammenheng. NAVs tjenester omfatter blant andre inntektssikring, arbeidsformidling, pensjon og trygdeytelser, helsetjenester, helserefusjon via trygden, praktisk bistand og forebyggende tiltak. NAVs hovedoppgave er å gjennomføre arbeidsmarkeds-, trygde- og pensjonspolitikken og forvalte tilhørende lovgivning. En viktig oppgave er å sikre rett ytelse til den enkelte og i tillegg følge opp og kontrollere tjenester, ytelser og utbetalinger, jf. lovens § 4, 1. og 2. ledd. Det er ikke minst NAVs kontrolloppgaver som gir opphav til viktige og aktuelle personvernspørsmål, se nedenfor.

16.5.5.1 NAV og taushetsplikt

Et av virkemidlene for å oppnå økt samarbeid og samordning av offentlige tjenester er prinsippet om én dør og en helhetlig tilnærming til brukeren på tvers av tidligere skiller og ulike systemer (trygd, sosialtjeneste, arbeidsformidling). I NAV-loven § 13, 1. ledd slås det fast at arbeids- og velferdsetaten og kommunene skal ha felles lokale kontorer i alle kommuner, og at disse kontorene skal ivareta oppgaver etter både trygde-, arbeidsmarkeds- og sosialtjenesteloven. Arbeids- og velferdsetaten og kommunen kan inngå avtale om at også andre av kommunens tjenester skal inngå i kontoret, jf. § 13, 2. ledd. Avtalen mellom arbeids- og velferdsetaten og kommunen kan også inneholde bestemmelser om å utføre oppgaver på hverandres myndighetsområder, se § 14, 2. ledd.

Taushetsplikten til de ansatte i NAV er regulert i lovens § 7. Det heter her at «Enhver som utfører tjeneste eller arbeid for Arbeids- og velferdsetaten etter denne loven, har taushetsplikt etter forvaltningsloven §§ 13 til 13 e.» Taushetsplikten omfatter også fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bosted og arbeidssted. Det presiseres at dette ikke er til hinder for at opplysninger om en person brukes ved formidling av arbeid eller ved gjennomføring av arbeidsmarkedstiltak.

Den nye forvaltningsenhetens virksomhet forutsetter innhenting og behandling av en stor mengde personopplysninger. Dette er i seg selv en utfordring i forhold til personvernet. Ikke minst den arbeidsevnevurdering som foretas av den enkelte som ledd i tiltak etter arbeidsmarkeds- og trygdelovgivningen forutsetter innhenting av sensitiv og omfattende informasjon om den enkelte. Av betydning i denne sammenheng er særlig at den nye store forvaltningsenheten er å oppfatte som ett organ i forhold til taushetsplikt. Dette følger av NAV-loven § 16, som slår fast at den enkelte ansattes taushetsplikt ikke er til hinder for at opplysninger er tilgjengelig for andre ansatte innen kontoret i den utstrekning som trengs for en hensiktsmessig arbeids- og arkivordning, blant annet til bruk ved veiledning i andre saker. Bestemmelsen har samme ordlyd som tilsvarende bestemmelse i forvaltningsloven § 13 b, 1. ledd nr 3, og må tolkes på tilsvarende måte. Bestemmelsen gir en ganske vid og åpen fullmakt til å formidle opplysninger til andre ansatte innenfor etaten og kommunens felles kontor. Kravet om nødvendighet («trengs») er ganske strengt og utgjør her en klar begrensning. Også kravet om hensiktsmessighet utgjør en grense med hensyn til hva som er legitime begrunnelser for å dele informasjon med andre ansatte innen etaten.

Personvernkommisjonen mener at de personvernrelaterte utfordringer her består i at etaten er stor og at «hensiktsmessighet» ofte vil kunne føre til at hele mapper gjøres tilgjengelige for andre ansatte i stedet for de enkelte relevante opplysninger. Det er derfor særdeles viktig at forvaltningsrettslige og personopplysningsrettslige rettssikkerhetsgarantier innfortolkes i regelverket knyttet til NAV-reformen (Bernt 2008), ikke minst kravet om nødvendighet. Det rettslige utgangspunkt er at taushetsplikten er en personlig plikt for den enkelte; «enhver som utfører tjeneste eller arbeid for et forvaltningsorgan», jf. forvaltningsloven § 13, 1. ledd. Den som har taushetsplikt skal hindre at «andre» får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om noens personlige forhold. «Andre» er i utgangspunktet også personer som arbeider ved samme kontor. Meddelelser eller tilgjengeliggjøring i form av adgang til journaler eller andre dokumenter, fysisk eller elektronisk, må dermed ha hjemmel i lov (ibid.), for eksempel bestemmelsene i forvaltningsloven. Forvaltningsloven § 13b, 1. ledd nr. 2 slår fast at taushetsplikt etter § 13 ikke er til hinder for at opplysninger brukes for å oppnå det formål de er gitt eller innhentet for, og blant annet kan brukes i forbindelse med saksforberedelse, avgjørelse, gjennomføring av avgjørelsen, oppfølging og kontroll. Dette, i tillegg til den nevnte bestemmelse i § 13 b, 1. ledd nr. 3 om nødvendighet og en hensiktsmessig arbeids- og arkivordning (som også står i NAV-loven § 16), er viktige stikkord i denne sammenheng og angir viktige

juridiske grenser for hva som kan anses som saklig, forsvarlig og velbegrunnet behandling av personopplysninger.

Samlet sett er det klart at NAV-loven åpner opp for en betydelig informasjonssirkulasjon innad i den store enheten som nå kalles arbeids- og velferdsforvaltningen. På det åpne møtet om personvern i helsesektoren, der også NAV-reformen sto på dagsorden, kom det også fram at brudd på taushetsplikten er et nokså velkjent fenomen. NAV har imidlertid iverksatt holdningsskapende og kompetansehevende tiltak for å begrense omfanget av dette og har også gjennomført en kampanje for personvern og informasjonssikkerhet som svar på kritikk som har fremkommet, blant annet fra Datatilsynet.

16.5.5.2 Opplysninger til andre organer

NAV-loven § 7, 2. ledd omhandler forholdet til andre forvaltningsorganer. Det følger av bestemmelsen at opplysninger til andre forvaltningsorganer bare kan gis «når det er nødvendig for å fremme etatens oppgaver[3] eller for å forebygge vesentlig fare for liv eller alvorlig skade på noens helse.» I denne sammenheng er «andre forvaltningsorganer» organer som ikke er en del av arbeids- og velferdsetaten, for eksempel sykehus og andre helseinstitusjoner. Alternativet om «nødvendig for å fremme etatens oppgaver» er skjønnspreget, men setter likevel grenser i forhold til usaklig og ubegrunnet informasjonsflyt som ikke er knyttet til oppgaver organet skal løse. «Nødvendig» er et ganske strengt vilkår, samtidig som det ikke vil være klart for alle hva som ligger i dette. Personvernkommisjonen antar derfor at det vil være behov for systematiske opplæringstiltak for å sikre en forsvarlig og ensartet oppfatning av hvilke opplysninger som kan formidles til andre organer.

NAV-loven legger ellers til rette for omfattende samarbeid og bistand mellom arbeids- og velferdsetaten og sosialtjenesten, og i den sammenheng åpnes det for vidtgående unntak fra taushetsplikten. Det heter i § 8 at arbeids- og velferdsetaten skal gi sosialtjenesten bistand i saker som gjelder den enkelte bruker og «skal av eget tiltak gi sosialtjenesten opplysninger» om forhold som bør føre til tiltak fra sosialtjenestens side, jf. § 8, 2. ledd. Det presiseres imidlertid at opplysninger bare kan gis etter samtykke fra brukeren eller med hjemmel i lov. Opplysninger om stønadssaker, ytelsessaker og arbeidsforhold kan imidlertid gis uten hinder av taushetsplikt, jf. 3. ledd, og må forstås slik at denne type opplysninger kan gis uavhengig av samtykke fra den enkelte. Sosialtjenesten på sin side plikter å gi opplysninger og bistand og avgi uttalelser til etaten uten hinder av taushetsplikt, jf. arbeidsmarkedsloven § 19 og folketrygdloven § 21-5. Personvernkommisjonen vil i lys av den omfattende informasjonsutvekslingen det her legges opp til fremheve behovet for oppfølging og kontroll med praktiseringen av lovverket for å sikre at formåls- og forholdsmessighetskravet som følger blant annet av EMK artikkel 8, ivaretas.

16.5.5.3 NAVs kontroll med helsetjenesten

Når det gjelder NAVs forhold til helsetjenesten, oppstår det her som på andre felt spørsmål om hvordan velferdsetatens behov for dokumentasjon og kontrolltiltak skal avveies mot hensynet til personvern. NAV vil kunne ha behov for konkrete medisinske opplysninger som grunnlag for vurderinger om rett til stønad i enkelttilfeller, og opplysninger som grunnlag for vurdering av helsepersonells praktisering av regelverket knyttet til trygderefusjon. Folketrygdloven § 21-4 gir NAV rett til å innhente nødvendige opplysninger fra behandlingspersonell og andre som yter tjenester for trygdens regning. De som gir behandling eller yter tjenester for trygdens regning plikter etter krav fra NAV å gi de erklæringer og uttalelser som er nødvendige for at etaten skal kunne vurdere rettigheter og plikter etter loven, jf. § 21-4, 2. ledd. I en legeerklæring om sykefravær plikter legen å opplyse om en sykdom eller en skade kan ha sammenheng med arbeidssituasjonen. NAV kan også pålegge helseinstitusjoner, fengsler og boformer for heldøgns omsorg og pleie å gi rutinemessige meldinger om innskriving og utskriving av klienter, jf. § 21-4, 3. ledd. De som slik blir pålagt å gi opplysninger, erklæringer og uttalelser til NAV, plikter å gjøre dette uten ugrunnet opphold og uten hinder av taushetsplikt, jf. folketrygdloven § 21-4, 4. ledd.

Et sentralt spørsmål er hva som er «nødvendige» opplysninger for å ivareta de aktuelle kontrollformål, og hvem som skal ta stilling til dette. Om dette hersker det både tvil og ulike oppfatninger. I juli 2007 sendte Arbeids- og inkluderingsdepartementet ut et forslag til tiltak mot trygdemisbruk på høring (se Ot.prp. nr. 76 (2007-2008)). Forsla-

[3] Dette alternativet er formulert etter samme lest som det vi finner i forvaltningsloven § 13 b, 1. ledd nr 5 («og ellers slike opplysninger som det er nødvendig å gi for å fremme avgiverorganets oppgaver etter lov, instruks eller oppnevningsgrunnlag»).

get ble oversendt til behandling i Stortingets Arbeids- og sosialkomité den 22. september 2008, og innstiling ventes i desember 2008. Forslaget fra Arbeids- og inkluderingsdepartementet møtte sterk kritikk, blant annet fra Datatilsynet, som karakteriserte forslaget som svært negativt for personvernet, fordi det etter tilsynets mening innebar nærmest en blankofullmakt til å innhente og videreformidle til dels svært sensitive personopplysninger (Datatilsynet 2007a). Ett av forslagene var å gi NAV nærmest ubegrenset adgang til fullstendige og uredigerte pasientjournaler. Datatilsynet fremhevet viktigheten av at bruk av pasientjournaler utenfor helsetjenesten begrenses til et minimum, at enhver forespørsel om utlevering må begrunnes og at bare relevante opplysninger kan utleveres. I den grad informasjon utleveres, er det viktig at pasienten er innforstått med dette. Datatilsynet påpekte det åpenbart problematiske ved at NAV gis videre adgang til pasientjournaler for å etterforske mulig trygdesvindel enn politiet har for å etterforske drap, og stilte spørsmål ved begrunnelsen for at NAV skulle ha videre fullmakter enn politi, forsikringsselskaper og arbeidsgivere. Datatilsynet fremhevet at alle unntak fra taushetsplikten må være begrunnet i helt spesielle forhold og at unntaket ikke må gå lenger enn det som er strengt nødvendig. Det påpekes at det er legen som kjenner journalen og derfor best kan vurdere hva som er relevant.

Personvernkommisjonen slutter seg til en slik nødvendighetsbegrensning, men antar at det i konkrete saker vil kunne være vanskelig å vite hva som er relevant før man har sett hva journalen inneholder. Dessuten er det ikke sikkert at legen alltid vet hva som er relevante opplysninger i forhold til ulike bestemmelser i trygde- og sosiallovgivningen.

NAV har i brev til Datatilsynet den 26. september 2007 gitt uttrykk for at en uredigert journal vil innebære omfattende sorteringsarbeid for saksbehandlerne og sjelden tilføre saken ytterligere relevante opplysninger (ibid.). Når det gjelder mistanke om trygdemisbruk fra legens side, anføres det imidlertid at situasjonen er annerledes, og at det i disse tilfeller ikke er forsvarlig at legen selv foretar vurderingen av hvilke opplysninger som er nødvendige etter folketrygdloven § 21-4. Når legen mistenkes for trygdesvindel, kan vedkommende selv ikke forestå vurderingen av hvilke opplysninger som er relevante. Datatilsynet fremhever det uheldige ved at intetanende pasienter får «brettet ut» hele sin sykehistorie fordi de har en lege som NAV har funnet det nødvendig å gå nærmere etter i sømmene. Det fremheves som et minimumskrav at NAV gir vedkommende pasient informasjon om at pasientjournalen ønskes innhentet, grunnen til at den ønskes innhentet, hvor lenge NAV trenger den og hvem som vil kunne lese den hos NAV. Personvernkommisjonen synes dette er rimelige krav. Datatilsynet nevner muligheten for å oppnevne en ekstern nemnd eller lignende for å vurdere hvilke opplysninger som er nødvendige før NAV får oversendt journaler. Personvernkommisjonen vil peke på at dette fører til at enda flere får innblikk i taushetsbelagte opplysninger, noe som i seg selv er uheldig. En bedre løsning vil være at kun én eller et begrenset antall personer i NAV gis adgang til å vurdere opplysningene med det formål å utøve nødvendig kontroll. Det vil i så fall innebære at tolkningen av NAV-loven § 16 om nødvendighet og hensiktsmessig arbeidsordning må presiseres nærmere med tanke på disse tilfellene.

16.5.6 Registre og de mange gode formål

Norge har mange registre sammenlignet med andre land. Formålet med registrene er at vi skal styre og administrere samfunnsoppgaver med større kunnskap, kvalitet, rasjonalitet og effektivitet. Dette er en opplysningstidsidé, særlig kjent fra Frankrike i tiden etter revolusjonen. Ved å samle informasjon i sentraliserte databanker og analysere disse dataene vitenskapelig, skulle man utvikle fornuftsbasert styringskunnskap og dermed et mer fornuftig og kunnskapsbasert styresett (Desrosières 2002). Norge har ikke minst brukt registre til medisinsk forskning og til å administrere sykdomsforebyggende programmer, for eksempel mammografiscreeningprogrammet. Det vil si at registrene bygges ut fra gode hensikter som administrasjon og vitenskapelig utvikling. Men registrene er ikke uproblematiske selv om hensiktene er gode.

I januar 2008 var det store oppslag om at organisasjonen «Privacy International» hadde gitt Norge en dårlig ranking ut fra en personvernvurdering (se f.eks. Aftenposten.no 2008b). Når vi gransker punktene som er basis for rankingen (Privacy International 2007) ser vi at en av kategoriene der Privacy International har plassert Norge lavt gjelder «overvåkning av helse, økonomi og forflytning». Her er det blant annet de mange medisinske registrene, samt mulighetene for koblinger mellom disse, som trekker ned.

16.5.6.1 Sentrale helseregistre

Det følger av helseregisterloven at det ikke kan etableres andre sentrale helseregistre enn det som følger av helseregisterloven eller annen lov, jf. § 8, 1. ledd. Loven gir selv hjemmel til opprettelsen av 9 sentrale helseregistre med direkte identifiserbare opplysninger som ikke bygger på samtykke fra de registrerte: Dødsårsaksregisteret, Kreftregisteret, Medisinsk fødselsregister, Meldingssystem for smittsomme sykdommer, Det sentrale tuberkuloseregisteret, System for vaksinasjonskontroll og Forsvarets helseregister, Norsk pasientregister og Nasjonal database for elektroniske resepter, jf. 8, 3. ledd.

Opprettelsen av andre sentrale helseregistre skal som hovedregel bygge på et samtykke fra de registrerte og kan reguleres i forskrift, jf. § 8, 2. ledd. Samtykke kan imidlertid unnlates i den grad det i forskriften bestemmes at helseopplysningene bare skal behandles i pseudonymisert eller avidentifisert form.

På tross av at samtykke er en klar hovedregel i helseregisterloven, viser det seg i praksis at flere og flere helseregistre opprettes uten borgernes medvirkning. Selv om disse registrene pseudonymiseres eller avidentifiseres i henhold til lovens krav, er det ikke alltid at dette alene kan imøtekomme de personvernulempene opprettelsen av registeret medfører. Det er heller ikke gitt at personvernhensyn ivaretas tilfredsstillende selv om registeret lovhjemles. Slike registre er i hovedsak direkte identifiserbare selv om identiteten krypteres. Det kan imidlertid stilles spørsmål ved om ikke formålet med registeret kunne vært oppfylt selv om registeret ble pseudonymisert.

I det følgende vil Personvernkommisjonen gå nærmere inn på to helseregistre som reiser særskilte personvernproblemer – Norsk pasientregister og IPLOS. Norsk pasientregister vil komme til å omfatte helseinformasjon om praktisk talt hele den norske befolkningen fra fødselen og livet ut, og må betraktes som er særlig sensitivt register, både i forhold til omfang og type opplysninger. Sentrale forskningsmiljøer har imidlertid motsatt seg pseudonymisering av registeret. IPLOS er et register over brukere av kommunale pleie- og omsorgstjenester. Dette registeret er pseudonymisert, men de registrerte har reist klager over andre personvernaspekter ved registreringen.

16.5.6.2 Norsk pasientregister

Helse- og omsorgsdepartementet foreslo i Ot.prp. nr. 49, (2005-2006) Om lov om endringer i Helseregisterloven (Norsk Pasientregister) at Norsk pasientregister (NPR) omdannes til et personidentifiserbart register, og at de registrerte data også kan benyttes i medisinsk og helsefaglig forskning og som datagrunnlag for sykdoms- og kvalitetsregistre. NPR har siden 1997 vært etablert som et avidentifisert register med konsesjon fra Datatilsynet.

Formålet med å opprette registeret var å kunne gi datagrunnlag for administrasjon, styring og finansiering av spesialisthelsetjenesten. Begrunnelsen for å omdanne registeret til et personidentifiserbart register var å ivareta behovet for bedre datakvalitet, av hensyn til administrative formål og av hensyn til mer effektiv styring, samt ut fra forskningsformål. Det var antatt at et personidentifisert register ville gi bedre muligheter for kvalitetssikring av data og dermed forbedre kvaliteten på helsetjenester, samt bidra til sikrere kunnskap om sykdommers årsak, forebygging og behandling (Ot.prp. nr. 49, (2005-2006), ss. 5-6).

Stortingets Helse- og omsorgskomiteen la den 16. januar 2007 fram sin innstilling (Innst. O. nr. 40, 2006-2007) om de foreslåtte endringer i Helseregisterloven. Komiteen var samstemt i oppfatningen om viktigheten av å kryptere identitetene i registeret, men var delt i synet på om krypteringen skal skje internt i registeret eller av en uavhengig instans. I en åpen høring på Stortinget den 12. oktober 2007 ble det fremmet advarsler mot å gjøre NPR til et personidentifiserbart register. Professorene Erik Boe og Dag Wiese Schartum viste til at et pseudonymt register ville kunne realisere formålet med registeret, samtidig som personverninteresser blir bedre ivaretatt. I høringsrunden har også Datatilsynet og KITH vært kritiske til forslaget, mens flere medisinske forskere har hevdet at muligheten for personidentifisering er avgjørende for registerets kvalitet og nytteverdi.

Personvernkommisjonen er av den klare oppfatning at pseudonymisering av helseopplysninger bør benyttes i så stor grad som mulig. Dette gjelder både for NPR og flere andre særlig sensitive helseregistre. Pseudonymisering som personvernfremmende tiltak bør ikke utelukkes uten at det er foretatt en grundig vurdering av fordeler og ulemper. Den tilbakeholdenheten som kan spores hos politikere og enkelte forskningsmiljøer når det gjelder pseudonymisering, kan tyde på problemer med å forstå hva pesudonymisering innebæ-

rer og forståelse for at de fleste formål med registrene kan realiseres på tross av tiltaket.

Personvernkommisjonen erkjenner at pseudonymisering er kostbart, både i forhold til etablering, vedlikehold og bruk. Dette bør imidlertid ikke være til hinder for at psedonymisering blir vurdert som et reelt alternativ ved etablering av helseregistre.

16.5.6.3 Særlig om IPLOS

Akronymet IPLOS står for Individbasert Pleie og Omsorgsdata. IPLOS er et register over alle brukere av og søkere til kommunale pleie- og omsorgstjenester. Ifølge Helsedirektoratet er formålet med IPLOS å «danne grunnlag for nasjonal statistikk for pleie- og omsorgssektoren. Det er et verktøy for dokumentasjon, rapportering og statistikk for kommunene og for statlige myndigheter» (Sosial- og helsedirektoratet 2005a). Tanken bak IPLOS er at saksbehandlingen forut for vedtak om pleie- og omsorgstjenester skal standardiseres gjennom bruk av et felles registreringsskjema. Skjemaet sørger for at visse målinger inngår i vedtaksgrunnlaget og målingsresultatene kan deretter tappes av til bruk i forskning om og forvaltningsmessig oppfølgning av tjenestene.

IPLOS ble først utredet av en arbeidsgruppe nedsatt av Sosial- og helsedepartementet i 1998 (Sosial- og helsedirektoratet 2007, s. 4). Allerede i mandatet (Sosial- og helsedirektoratet 2000) var det klart at IPLOS skulle bli et obligatorisk register. Arbeidsgruppen var gitt i mandat å «komme fram til hvilke opplysninger staten skal pålegge alle kommuner å samle inn» samt «gi entydige definisjoner av datasettet» for en individbasert pleie- og omsorgsstatistikk i KOSTRA (kommune stat rapporteringen) (Sosial- og helsedirektoratet 2000, s. 5). Arbeidsgruppen besto av representanter fra fylkeslegene, fylkesmennene, departementer, Kommunenes sentralforbund, forskere, Statistisk sentralbyrå, kommuneadministrasjoner, ansatte i eldreomsorgen og Sosial- og helsedepartementet. Det var imidlertid ingen representanter for organisasjoner av og for grupper som mottar helse- og omsorgstjenester. IPLOS ble utredet gjennom flere utvalg og passerte flere utviklingstrinn (se f.eks. Sosial- og helsedirektoratet 2003, Sosial- og helsedirektoratet 2005b, Lynne 2007, Lynne og Voldsund 2007), uten at de tenkt registrerte var representert i prosessen og uten at man satte spørsmålstegn ved personvernaspekter ved eller nytteverdi av systemet. Det synes å ha blitt tatt for gitt at mer detaljerte opplysninger gir bedre kunnskapsgrunnlag og i sin tur bedre tjenester, at hjemmel var alt som trengtes for at et nytt personregister kunne aksepteres, og at det eneste som trengte utredning dermed var tekniske og formelle aspekter (for eksempel hvordan spørsmål formuleres, om svaralternativer skal deles i fire eller fem nivå, hvilke tabeller som skal produseres), systemopplæringstiltak, samt estimerte kostnader for systemet. Riktignok ble noen IPLOS-registrerte intervjuet i forbindelse med utprøving av systemet (Lynne og Voldsund 2007). Et hovedfunn fra intervjuene var at på spørsmålet «Hva vet du om IPLOS?» svarte åtte av de ti intervjuede «Jeg har ikke hørt om IPLOS» (Lynne og Voldsund 2007, s. 6). Det var først i 2006, da IPLOS ble innført på landsdekkende basis og de første IPLOS-statistikkene ble publisert, at organisasjoner for mennesker med ulike funksjonsnedsettelser ble oppmerksom på systemet og protesterte. Og det var først etter disse protestene at Sosial- og helsedirektoratet nedsatte en IPLOS-arbeidsgruppe, der noen av de berørte organisasjonene ble representert. Denne gruppen fikk i mandat å videreutvikle IPLOS, samt å vurdere IPLOS i forhold til «etikk, rettssikkerhet og personvern; hjemmelsgrunnlaget [… og] lokal, regional og nasjonal nytteverdi, herunder en samlet kost/nytte-analyse av foreslåtte endringer» (Sosial- og helsedirektoratet 2008).

Visse endringer ble gjort i IPLOS etter at arbeidsgruppens rapport ble offentliggjort, men organisasjoner har fortsatt å protestere. Hva er det de protesterer på? Personvernkommisjonen vil særlig trekke fram tre forhold:

For det første klager IPLOS-registrerte over personopplysningsvernet i IPLOS. Riktig nok er IPLOS et av Norges få pseudonymiserte helseregistre, men om pseudonymisering er aldri så ønskelig som personvernforbedrende tiltak (NOU 1993:22), må den ikke bli en sovepute. Heller ikke aggregering er garanti for et tilstrekkelig personopplysningsvern i det enkelte tilfellet. At et register er pseudonymt og at data kun slippes ut til offentligheten i aggregert form, gir begrenset beskyttelse for registrerte med sjeldne trekk. Med andre ord, navn og personnummer er ikke de eneste lett personidentifiserbare opplysninger i IPLOS-systemet. Diagnose, alder, sivilstand eller bruk av et bestemt hjelpemiddel, kan være like personavslørende hvis det er tilstrekkelig sjeldent innenfor et gitt område der en aggregert rapport genereres (en bydel, en kommune, et fylke, i enkelte tilfeller kanskje hele landet).

For det andre klages det over at myndighetene har hoppet delvis bukk over samtykkeprinsip-

pet og vært sent ute med medvirkningstiltak. Brukermedvirkning har man hatt, men bare fra brukere av de tiltenkte statistikkene til forvaltnings- og forskningsformål. Brukere av tjenestene som er tenkt registrert i IPLOS ble ikke tatt med på råd før de protesterte over utformingen av IPLOS og forlangte plass ved forhandlingsbordet.

Medvirkning skal også gjelde på mikronivået i den daglige driften av IPLOS-systemet. Det er meningen at den registrerte selv skal delta i registreringsprosessen. Men også her har det sviktet. Registrerte fra flere kommuner har klaget over at de er blitt IPLOS-registrert i det stille, uten at de selv har vært klar over det, og at de til dels ikke kjenner seg igjen i de data som er registrert om dem (Tøndel under utgivelse). Ved å gjøre registreringen pliktig og pseudonymisert, har samtykkeprinsippet blitt satt til side. Man har heller ikke hatt en konsekvent praksis der deltakelse i registreringsarbeidet kunne utgjøre en form for samtykke, om ikke samtykke i selve registreringen så i alle fall medvirkning på registreringens innhold. I følge noen av de registrerte, har dette gitt utslag ikke bare i en følelse av svekkede borgerrettigheter, men også i dårlig datakvalitet.

For det tredje klages det over at den grunnleggende strukturen i IPLOS, med sitt individfokus, bygger på en forståelse av funksjonshemming som de registrerte tar avstand fra. Når det gjelder forståelsen av ulike funksjonshemminger, er det to tilnærminger som står i motsetning til hverandre. Det ene, og kanskje vanligste, er at funksjonshemmede lider av noen skader eller mangler som gjør at de ikke kan tilpasse seg «normale» omgivelser. Mange interesseorganisasjoner for såkalt «funksjonshemmede» fremmer en motsatt forståelse. Deres tilnærming tar opp i seg at de fleste opplever slike tilpasningsproblemer en eller flere ganger i løpet av sitt liv. Vi brekker benet og får dermed bevegelsesproblemer i en periode; vi er småbarnsforeldre og sliter med å dra barnevognen over fortauskanter og snøskavler; vi eldes og sliter med nedsatt syn og hørsel. Altså er det ikke bare normalt, men universelt å oppleve ulike former for funksjonshemminger i løpet av livet. Da blir det ulogisk å definere fravær av skader og funksjonsproblemer som «normalt». Men problemene forsvinner ikke av den grunn. Følgelig bør fremstillingen være at det er omgivelsene som er mangelfulle i og med den mangelfulle tilpasningen til individers mangfoldige behov. Det oppleves da som problematisk at IPLOS nettopp er «individbasert» og fremstiller den enkelte som «unormal». Det blir også et problem at IPLOS ikke registrerer samtlige brukere av kommunale tjenester (for eksempel snøbrøyting, skole, renovasjon), men kun registrerer brukere av omsorgstjenester, altså av tjenester som hjelper til å bøte på omgivelseshindre. I selve sin oppbygging knytter IPLOS manglene til et mindretall individer. For IPLOS-registrerte som tilslutter seg bildet av at problemene sitter i omgivelsene og gjelder oss alle, oppleves derfor IPLOS-registrering som et overgrep mot verdigheten, mot retten til å betrakte seg som normal: Ved at IPLOS-data registreres som trekk ved individet, blir individene også sittende igjen med opplevelsen av å være stigmatisert. Dette gjaldt særlig den første landsomfattende utgaven av IPLOS, der formuleringer på enkelte funksjonsspørsmål ble opplevd som svært krenkende, særlig spørsmål om hvorvidt den registrerte «spiser mat på en kulturelt akseptabel måte» «har intimhygiene ved menstruasjon», «tørker seg nedentil og vasker hender», og «kler seg sosialt akseptabelt». De mest krenkende formuleringene ble endret av arbeidsgruppen nedsatt i 2006 for å videreutvikle IPLOS (Sosial- og helsedirektoratet 2008). I denne arbeidsgruppen var organisasjoner for mennesker med funksjonsnedsettelser representert. De formuleringene de registrerte reagerte mest på, ble endret, men fortsatt oppleves enkelte formuleringer som krenkende, og både nye og gamle formuleringer benyttes fortsatt retorisk i de registrertes kamp mot IPLOS (se f.eks. http://www.alldifferent-allequal.no/?sid=64).

Personvernkommisjonen vil avslutningsvis i denne sammenheng knytte noen betraktninger til proporsjonalitet, som er sentralt i personvernsammenheng. Personvernkommisjonen legger til grunn at det i mange tilfeller vil kunne gjøres inngrep i personvernet. Her som ellers må hensynet til og behovet for personvern vurderes opp mot andre legitime hensyn og behov i samfunnet. Personvernet må imidlertid anses som såpass verdifullt at det ikke kun utgjør en salderingspost som må vike for ethvert annet hensyn. Når det gjelder IPLOS, og tilsvarende også for alle andre helseregistre, må personvernet avveies mot tunge verdier som helse, forskning, og effektivitet i Norges største offentlige sektor. Disse verdiene bør da ikke legges i vektskålen som påstander uten klare og konkrete begrunnelser. Snarere må det forventes klar dokumentasjon som grunnlag for legitimitet. Oppnår vi virkelig bedre og mer effektive helsetjenester ved å samle og bearbeide de dataene som IPLOS registrerer? De registrerte

bestrider dette. Ut fra deres forståelse av funksjonsnedsettelse, er det feil data som etterspørres, og ut fra deres erfaringer er det mange datafeil i registeret. På personvernsiden av vektskålen bør man ikke bare påstå, men også dokumentere, at registeret har så lave personvernkostnader som mulig. Her er det et positivt trekk at IPLOS er et pseudonymisert register. Men de registrerte påpeker at det likevel er så mange detaljer i registeret og så mye kopling mellom disse i publikasjonene at registrerte individer blir lett identifiserbare. Dessuten påpeker de som nevnt at registeret oppleves krenkende på andre måter (stigmatisering, uhensiktsmessige data, se ovenfor) og ikke minst ved at registeret er utformet slik at det uttrykker et syn på funksjonsnedsettelse som i seg selv er krenkende. Altså mener de registrerte at balansen mellom verdier og interesser blir for skjev – personvernkostnaden er stor mens nytteverdien for forskning og forvaltning er liten.

16.6 Kommisjonens anbefalinger og forslag til tiltak

Mange av de foreslåtte tiltakene under dette avsnittet handler om å sikre at regelverkets bestemmelser om taushetsplikt ivaretas i praksis. Overholdelse av taushetsplikten er selve fundamentet for et fortsatt tillitsforhold mellom helsetjeneste og pasient. Dersom dette fundamentet svekkes, vil pasientenes personvern stadig være truet. Pasienten må kunne stole på at opplysninger om helse og andre personlige forhold ikke kommuniseres videre, ellers mister vedkommende kontroll over sensitive opplysninger om egen person.

Tiltak knyttet til taushetsplikten vil særlig omtales i avsnittene 16.6.1, 16.6.5 og 16.6.7 nedenfor, deretter kommer tiltak som gjelder andre forhold ved helsetjenesten.

16.6.1 Kommunikasjon med pasienter

Personvernkommisjonen vil fremheve behovet for å sikre konfidensialitet i kommunikasjonen mellom pasient og behandlingspersonell. Også pasienter som ligger på rom med flere har krav på taushet om sine personlige forhold. Det må innføres nye rutiner for å sikre retten til at sensitive helseopplysninger ikke formidles i påhør av andre. Den tradisjonelle legevisitten bør reformeres på en slik måte at taushetsplikten ivaretas.

16.6.2 Utelatelse av individualiserende kjennetegn

Etter helsepersonelloven § 26 skal opplysninger eller journalutdrag i samband med internkontroll «så langt det er mulig, gis uten individualiserende kjennetegn». På dette området mener Personvernkommisjonen at det bør gjennomføres tiltak for å sikre at personvernhensyn ivaretas i tråd med lovgivers intensjoner. De tekniske mulighetene elektronisk pasientjournal (EPJ) faktisk gir for pseudonymisering og andre metoder for å skjule identitet bør utnyttes fullt ut. Standarden for EPJ bør utvikles slik at individualiserende kjennetegn ved enkle grep kan erstattes med automatisk genererte pseudonymer.

Personvernkommisjonen anbefaler videre at klageinstanser i helsesektoren, inklusive Helsetilsynet, går gjennom sin praksis i forhold til å utelate identifiserende kjennetegn i klagesaker.

I denne sammenhengen er såkalt immunisering av søkemotorer et aktuelt tiltak (se omtale i avsnitt 10.1.4.

16.6.3 System for identitetsadministrasjon

Som en videreutvikling av automatisk pseudonymisering av individualiserende kjennetegn (jf. avsnitt 16.6.2) kan det være aktuelt å knytte slik pseudonymisering til et system for identitetsadministrasjon (se avsnitt 10.2 om personvernfremmende teknologier). Dette muliggjør sammenkobling av registre uten at personlig identitet avsløres, eller studier der man følger et individ over tid og på tvers av registre og journaler, uten at dette individet kan identifiseres gjennom individualiserende kjennetegn eller på annen måte.

Det er krevende å få til velfungerende systemer av denne type, men Personvernkommisjonen mener at arbeidet med å få på plass gode systemer for identitetsadministrasjon innen helsesektoren bør ha høy prioritet. Å imøtekomme helsevesenets behov for administrasjon, kontroll og styring ved å åpne opp for en stadig mer omfattende bruk av personidentifiserbar informasjon er etter kommisjonen oppfatning ikke akseptabelt.

16.6.4 Personvernvennlig bruk av elektronisk pasientjournal (EPJ)

Personvernkommisjonen har observert at systemene og den programvaren som i dag er i bruk i helsetjenesten ikke alltid anvendes på en måte som ivaretar taushetsplikten innad i den enkelte

virksomhet. Her er det nødvendig med personvernfremmende tiltak både med tanke på utvikling av tilfredsstillende programvare, rutiner og annet av betydning for faktisk etterlevelse av taushetsplikten. Mulighetene for tekniske og menneskelige feil må begrenses og IKT-bruken må tilpasses helsetjenestens krav, ikke minst bestemmelsene om taushetsplikt og behovet for tilgangskontroll.

Personvernkommisjonen vil fremheve behovet for en grundig gjennomgang av personvernhensyn før det gis adgang til tilgang til EPJ på tvers av foretak. Det må sørges for ivaretakelse av taushetsplikt og personvernhensyn før det kan åpnes for eksternt innsyn i pasientjournaler. Pasienten bør dessuten ha reservasjonsrett mot slikt eksternt innsyn.

16.6.5 Gjennomgang av reglene for taushetsplikt

Unntakene fra taushetsplikten er mange, og det foreligger etter Personvernkommisjonens mening en reell fare for at taushetsplikten blir uthulet uten at dette i seg selv har vært gjenstand for overveielse og utredning. Personvernkommisjonen vil anbefale at bestemmelsene om taushetsplikt gjennomgås med tanke på å evaluere hvorvidt dagens regelverk samlet sett innebærer en tilstrekkelig ivaretakelse av sentrale personvernhensyn.

16.6.6 Forbedring av pasienters rett til innsyn i journallogg

Som ledd i å hindre uberettiget innsyn i pasienters journaler støtter Personvernkommisjonen forslaget om at retten til innsyn i tilgangsloggen til pasientjournalen lovfestes. Det bør videre stilles konkrete krav til hva loggen skal inneholde, og den må være skrevet på en slik måte at pasienten selv kan forstå hvem det er som har vært pålogget journalen, når påloggingen er gjort, begrunnelsen for påloggingen og hvilke aktiviteter den påloggede har utført.

16.6.7 Opplærings- og holdningsskapende tiltak, innføring av bedre rutiner

Personvernkommisjonen mener det foreligger et klart behov for systematiske opplæring- og holdningsskapende tiltak og bedrede rutiner for å sørge for at taushetsplikten etterleves i praksis. Ikke minst gjelder dette lovgivningens krav om at det er de som har saklig behov for opplysninger om den enkelte pasient for å yte helsehjelp som skal ha tilgang til pasientens journal. Tilgangen til pasientjournaler har i praksis vært for vid, og det er derfor nødvendig med en innsnevring, slik at kun de som har et legitimt tjenstlig behov for opplysninger om den enkelte pasient har mulighet for faktisk innsyn.

Videre må kunnskapen om, og respekten for, taushetsplikten bedres innen helsetjenesten, slik at pasientenes rettmessige behov for diskresjon blir tilstrekkelig ivaretatt. Det eksisterer ikke, slik som mange helsearbeidere ser ut til å tro og praktisere, egne fora hvor taushetsbelagt informasjon kan utveksles fritt med andre så sant også disse har taushetsplikt. Gjennom tilsyn er det innen visse områder avdekket ulovlig praksis på dette området. Det er derfor svært viktig at helsepersonell gis grundig opplæring i reglene om taushetsplikt, ikke minst bestemmelsen i helsepersonelloven § 25, 1. ledd om at det bare kan gis opplysninger til samarbeidende helsepersonell og bare i den grad dette er nødvendig for å kunne gi forsvarlig helsehjelp.

Personvernkommisjonen tror at et enda større fokus på taushetsplikt og personvern i grunnutdanningen for personell i helse- og sosialsektoren vil være et effektivt virkemiddel i denne sammenheng.

Opplærings- og holdningsskapende tiltak, samt innføring av bedre rutiner, er også nødvendig i forhold til å redusere «snoking» i journalen. Helsepersonell må bevisstgjøres om viktigheten av at «snoking» ikke finner sted og om hvilke konsekvenser avsløring av urettmessig journalinnsyn kan få. Alle helseforetak bør ha fokus på dette i sitt kvalitetssikringsarbeid. Personvernkommisjonen mener en viktig del av lederansvaret ved helseinstitusjonene består i å skape en arbeidskultur med bevissthet om, respekt for og etterlevelse av regelverket om personvern, herunder håndtering av pasientinformasjon i ulike situasjoner.

Opplæring av ansatte og bevisstgjøring om hva som kan krenke personvernet er også påkrevd når det gjelder offentliggjøring av taushetsbelagt informasjon i postjournaler med den følge at personer kan identifiseres gjennom mediene. Her må det innføres rutiner som sikrer at den enkelte ikke kan identifiseres og at taushetsplikten overholdes.

16.6.8 Personvernfremmende tiltak ved opprettelsen av nye registre

Personvernkommisjonen har merket seg kritikken mot helseregisterloven når det gjelder ivaretakelse av personvernhensyn ved opprettelsen av helsere-

gistre. Personvernkommisjonen mener generelt at det er grunn til større årvåkenhet med hensyn til etablering av registre, både rene helseregistre og de forskningsregistre som i fremtiden vil bli opprettet i medhold av helseforskningsloven.

Det bør foretas grundige utredninger før helseregistre etableres. Det er ikke tilstrekkelig at registeret kan sies å tjene et godt formål. I tillegg må konsekvensene for personvernet utredes, og det må kunne dokumenteres at disse ikke er så negative at man av den grunn bør avstå fra å opprette registeret. Dersom man kommer til at registeret bør etableres, må det tilstrebes å gjøre bruken av registeret så personvernvennlig som mulig, for eksempel gjennom pseudonymisering eller andre metoder for identitetsbeskyttelse. Her mener kommisjonen at Grunnlovsfesting av personvernet (se kapittel 19) vil kunne bidra til en bedre balanse i vektleggingen av personvernhensyn opp mot andre interesser når helseregistre skal opprettes.

Dessuten må man erkjenne at omfang og bruk av etablerte helseregistre vil være i dynamisk utvikling. Derfor bør ethvert register undergis periodisk ettersyn og en revurdering, som bør være bygget inn i betingelsene for registerets hjemmel i form av en såkalt «solnedgangsklausul». Ved jevne mellomrom bør registeret opp til ny vurdering, der balansen mellom personvernet og andre interesser revurderes før hjemmel for registeret eventuelt forlenges. I forbindelse med revisjonen må det godtgjøres at registeret fremdeles har en nytteverdi og har vist seg egnet til å oppfylle det angitte formålet før det gis en forlengelse av hjemmelsgrunnlaget.

16.6.9 Gjennomgang av dagens helseregistre

Personvernkommisjonen vil foreslå en gjennomgang av alle etablerte sentrale helseregistre, med et klart fokus på personvern. Det bør foretas en utredning av hvorvidt de eksisterende registre har en berettiget eksistens og om det finnes registre med overlappende funksjon og formål. Personvernhensyn tilsier at registeromfanget begrenses til det som er nødvendig. Det bør også vurderes om ikke pseudonymisering er et tiltak som kan tas i bruk for langt flere helseregistre enn det som er tilfelle i dag.

Kommisjonen foreslår at det vedtas et moratorium mot etablering av nye helseregistre før denne gjennomgangen er fullført.

Kapittel 17
Personvern i transport og kommunikasjonssektoren

17.1 Hvordan utfordrer samferdsel personvernet?

Samferdsel dreier seg dypest sett om ulike måter å oppnå kontakt mellom mennesker på. Samferdsel innebærer kontakt gjennom fysisk forflytning ved hjelp av bil, tog, båt, fly mv. Det innebærer videre kontakt via post, telefon og Internett. Den førstnevnte kontaktformen går vanligvis under navnet transport, den andre under navnet kommunikasjon. Disse kontaktformene er på visse måter ulike og representerer forskjellige utfordringer, men i praksis er det betydelig overlapp mellom dem.

Transport og kommunikasjon utgjør vesentlige deler av et moderne samfunn. Samlet sett kan de samtidig utfordre de aller fleste dimensjonene ved personvernet gjennom krav til effektivitet, trafikk- og samfunnssikkerhet og bekjempelse av kriminalitet. Hvis vi betrakter personvernet fra et integritetsperspektiv (jf. kapittel 4.1) er det først og fremst enkeltindividers kommunikasjons- og informasjonsintegritet som blir satt på prøve ved samferdsel. Kommunikasjonsintegritet trues bl.a. av brevbrudd og avlytting av private samtaler, mens informasjonsintegritet trues bl.a. av uønsket spredning av fortrolig informasjon til andre. Samferdsel utfordrer også personers kroppslige og psykiske integritet. Undersøkelser av kroppen gjennom bruk av skanningsinnretninger ved grensekontroll (omtalt i avsnitt 17.4.1 nedenfor) er et eksempel i så måte. Kroppsskanning kan oppleves som krenkende i forhold til personers fysiske legeme, samtidig som den kan ramme den enkeltes selvbilde eller medføre andre følelsesmessige belastninger. Samferdsel kan dessuten sette territorial integritet under press – eksempelvis når den personlige sfære en passasjer får tildelt ved en sovekupé eller flysete som han/hun er tillatt å benytte som følge av kjøp av tog- eller flybillett, blir utfordret av medpassasjerers fysisk nærhet. Personvernkommisjonen går imidlertid ikke nærmere inn på dette aspektet ved personvern.

I hvilken grad samferdsel utfordrer personvernet, vil selvsagt variere i forhold til samferdselsform og andre omstendigheter. Som vi utdyper nedenfor kan forskjellige sikkerhetsstrategier i samband med samferdsel utgjøre en betydelig trussel mot personvernet. Hvorledes disse er innrettet, har betydning for hvilke sider ved personvernet som blir satt under press. Sikkerhetsstrategier er i hovedsak innrettet på tre forskjellige måter. Én fokuserer på kontroll og sikring av bestemte objekter/gjenstander (gods, bagasje, transportinfrastruktur mv.) for å lokalisere og fjerne uønskede objekter (våpen, sprengstoff mv.); en annen på overvåkning og kontroll av personer (primært antatt potensielle kriminelle); og en tredje på forebygging av ulykker og utilsiktede hendelser. I utgangspunktet medfører hver strategi ulike konsekvenser for personvernet. Lokalisering av objekter vil eksempelvis ofte kreve fysisk kontroll av personer (for eksempel flypassasjerer og flypersonell) og dermed utfordre personvernet i betydning vern av kroppslig og psykisk integritet. Overvåkning av personer vil derimot ha konsekvenser først og fremst for kommunikasjons- og informasjonsintegritet, og dermed personopplysningsvernet (jf. også Bjørnskau et al. 2007, ss. III-IV).

Graden av allmenn aksept for slike strategier – og dermed graden av personvernkrenkelse – vil også variere i forhold til samferdselsform og andre omstendigheter. Empiriske undersøkelser av folks holdninger til personvern og sikkerhet viser generelt at folk flest synes å akseptere en betydelig grad av kontroll og overvåkning dersom de føler at slike tiltak gjør hverdagen tryggere (jf. eksempelvis Teknologirådet 2007c). Etter terrorangrepene i USA den 11. september 2001, Madrid den 11. mars 2004 og London den 7. juli 2005 har graden av aksept nok økt. Samtidig ser vi at samferdselsform kan ha betydning for hvor mye kontroll folk aksepterer: Det synes for eksempel å være større aksept i Norge for relativt inngripende kontroll- og overvåkningstiltak ved flyplasser enn ved jernbanestasjoner (jf. Teknologirådet

2007c). Men det synes samtidig å være forholdsvis stor skepsis til innføring av sikkerhetsteknologier som retter seg mot kroppens intimsfære (jf. Teknologirådet 2007b, s. 27). Mange undersøkelser av folks personvernholdninger kan imidlertid være beheftet med metodiske svakheter, slik at en skal være forsiktig med å trekke bastante konklusjoner ut fra dem.

Samferdsel utfordrer ikke bare personvernet. I den grad for eksempel personopplysninger som er registrert i forbindelse med samferdsel blir brukt av offentlige myndigheter til å treffe avgjørelser som medfører begrensninger av den enkeltes autonomi eller andre rettigheter, blir handlingen ikke bare et person(opplysnings)vernmessige anliggende, men også et spørsmål om rettssikkerhet.

Uansett reise- eller kommunikasjonsmåte, enten det er til sjøs, med jernbane, i luften, på veien eller på Internett, blir vi i økende grad registrert på en eller annen måte. Dette er et hovedtrekk ved utviklingen av samferdselssektoren. Samferdselsområdet er også preget av den raske teknologiske utviklingen som åpner for stadig større muligheter for registrering, sporing og lagring av data, inklusiv personopplysninger. Denne muligheten benyttes i relativt stor utstrekning.

Krav til sikkerhet utgjør en viktig begrunnelse for at dette skjer. Sikkerhetshensyn ligger også bak en rekke andre tiltak innen samferdselssektoren som setter personvernet under press. Sikkerhet er imidlertid et noe upresist begrep som rommer to ulike aspekter. Det ene aspektet omhandler vern mot handlinger som har til hensikt å skade personer, organisasjoner eller stater (ofte uttrykt ved bruk av det engelske begrepet «security»). Det andre aspektet dreier seg om vern mot skade som er utilsiktet (uttrykt ved det engelske begrepet «safety»). I det følgende bruker vi «sikkerhet» i utgangspunktet som betegnelse på begge aspekter, men gjør presiseringer hvor det er nødvendig. Referanser til «trafikksikkerhet» skal imidlertid forstås som tiltak som først og fremst gjelder «safety»; referanser til «transportsikring» skal forstås som tiltak som primært gjelder «security» (jf. også Schartum 2007 som anvender en lignende begrepsbruk).

Sikkerhetskrav er ikke de eneste begrunnelsene for samferdselsrelaterte tiltak som utfordrer personvernet. En rekke andre krav gjør seg gjeldende – bl.a. krav til effektivitet, fortjeneste og planlegging. I det følgende gir vi eksempler på ulike tiltak som stammer fra disse kravene (inklusiv sikkerhetskrav) og som reiser særlige betenkeligheter fra et personvernperspektiv.

17.2 Effektivitetsmessige krav

Samfunnets økende kompleksitet stiller store krav til effektivitet og at alt skal fungere uten avbrudd. Det er et allment ønske om at samferdsel skal foregå på en mest mulig smidig måte. Dette medfører bl.a. økende bruk av elektroniske billetter, elektronisk registrering i bomringer og elektroniske betalingsformer (eksempelvis AutoPASS). Dette medfører i sin tur at en som reisende legger igjen mange elektroniske spor – og i økende grad, uansett hvilket transportmiddel som brukes.

Ved hjelp av elektroniske billetterings- og betalingssystemer, GPS (Geographical Positioning System), videokameraer osv., blir detaljerte opplysninger om den enkeltes bevegelser tilgjengelige. Følgende spørsmål blir stadig lettere å besvare:

- hvor er du? (geografisk lokalisering)
- når er du der? (tidspunkt)
- hvordan kommer du deg dit? (reisemåte)
- hva gjør du der? (aktiviteter)

AutoPASS-systemet representerer i så måte mange utfordringer. De helautomatiske bomstasjonene innebærer at hver passering av en bomstasjon blir registrert. Det foreligger imidlertid et noenlunde sporfritt alternativ der passeringsdata kun lagres i 72 timer før sletting, men informasjon om dette alternativet er gjort lite synlig av selskapene som driver bomstasjonene. Også lite synlig – i hvert fall inntil nylig – er informasjon om hva som lagres, hvor dataene lagres og deres bruksformål. Sistnevnte er særlig relevant i forhold til bekymringer vedrørende formålsutglidning (jf. kapittel 4.4.1). I denne sammenhengen er det verdt å merke at en utvidet bruk av AutoPASS for eventuelt å benytte systemet til ulike former for trafikkstyring og parkeringsformål er under evaluering i Vegdirektoratet. Videre vurderer Samferdselsdepartementet om det skal foreslås at skattemyndighetene rutinemessig får tilgang til passeringsdata.

En viktig del av AutoPASS tekniske plattform er RFID (nærmere beskrevet i kapittel 9.4). RFID anvendes i stadig flere sammenhenger, både innen og utenfor samferdselssektoren. I tillegg til bruk i «køfri-brikker» for passering av bomringer er RFID bl.a. innebygd i bilnøkler som elektronisk startsperre. Ved godstransport mv. er RFID-brikker i økende grad anvendt som erstatning for tradisjonelle strekkoder til logistikkformål. RFID innebærer samtidig muligheter for overvåkning og kontroll, uten at den som kontrolleres nødvendigvis er klar over det.

I denne sammenheng er det naturlig å nevne det såkalte EFC-direktivet (direktiv 2004/52/EF) som legger opp til samordning av betalingssystemer på vei i EU/EØS-området. Målet er at den enkelte bilist skal kunne inngå en AutoPASS-lignende avtale med et selskap og deretter kunne bruke den tildelte køfri-brikken i alle betalingsanlegg på tvers av landegrenser. Enkelt og effektivt for bilistene, sannsynligvis også for selskapene – og selvfølgelig med store muligheter for lagring og sporing av data om de samme bilistene. EFC-direktivet er imidlertid et rammedirektiv, og detaljene ved hele systemet er ennå ikke fastlagt. Direktivet er heller ikke innlemmet i EØS-avtalen, men anses for å være EØS-relevant.

17.3 Trafikksikkerhetsmessige hensyn

Ny teknologi kan gi oss mer effektive metoder til å forebygge farlig adferd i trafikken. For eksempel bygger nå de fleste bilfabrikantene inn flere førerstøttesystemer i bilene de produserer. Ett element i slike systemer er en «kjøreregistrator» («black box»), som blant annet kan registrere hvordan den enkelte bil er kjørt. Tanken bak registrering av disse dataene er å motvirke alvorlige konsekvenser av ubevisste førerfeil. Noen personer bryter imidlertid bevisst samfunnets kjøreregler, og ved hjelp av slike installasjoner vil en kunne få en mulighet til å stanse disse personene før de skader seg selv og andre i trafikken. Det er imidlertid betydelig usikkerhet rundt de rettslige rammene for bruk av dataene som blir generert. Hvem eier dataene? Dette kan bl.a. være et interessant spørsmål ved salg av et kjøretøy. Vil den første eieren ha mulighet til å slette dataene ved eierskifte? Hvem skal få tilgang til dataene og under hvilke omstendigheter? Forsikringsselskaper i forbindelse med skadeoppgjør, eller forut for aktuelle tilfeller av skade?

Mens eksisterende kjøreregistratorer primært retter seg mot kontroll med bilen, er det nylig blitt reist forslag fra en forsker som går i en annen retning. Forslaget går ut på å påby at alle biler skal utstyres med en registreringsenhet med navnet «adferdsboks», som skal registrere ulike aspekter ved førerens adferd. Denne boksen vil i følge forslaget eies av Statens vegvesen, være montert og plombert av godkjent verksted, registrere kjøreadferd og oppbevare loggene over lengre tid (Andresen 2007). Politiet vil kunne få adgang til loggene ved trafikkontroll. Boksen vil også kunne regulere kjøreadferd mer direkte, ved eksempelvis å gi lydsignal dersom bilføreren overskrider tillatt hastighet. Ulike «overskridelsesprofiler» tilpasset sjåførens alder mv. vil kunne programmeres inn. Strengere grenser vil da kunne anvendes overfor yngre bilførere eller førere som nylig er blitt tatt for trafikkforseelser. Etter forslaget trenger systemet ikke å logge bilens posisjon. Flere andre trekk ved det skisserte systemet vil imidlertid reise store personvernmessige bekymringer – ikke minst grunnet gjen- og misbrukspotensialet i forhold til de registrerte dataene. Adgang til loggene vil utvilsomt være ettertraktet ikke bare av politiet, men også andre (f.eks. forsikringsselskaper, bilfabrikanter og, i visse tilfeller, media).

Det vil være høyst relevant å trekke personvernhensyn inn i vurderingen av et eventuelt pålegg om slike systemer i kjøretøyer. Et slikt pålegg vil trolig kreve lovendring og at man tar stilling til hvordan opplysningene om kjøreadferd skal kunne brukes. Skal de for eksempel kunne brukes i retten og/eller for å kunne gripe inn før det skjer en ulykke, eller kun som grunnlag for statistikk?

En annen satsing som har trafikksikkerhet som hovedmål er Europa-kommisjonens «eCall»-initiativ, som tar sikte på å muliggjøre satellittsporing av biler ved bruk av GPS-enheter innebygd i bilene (jf. Europa-kommisjonen 2008). Systemet vil også gjøre det mulig for automatisk varsling fra biler om sted og omfang av trafikkulykker, og innebærer automatisk oppringning til nødmeldingssentral. Sammen med en rekke EU-medlemsland, Sveits og Island, har Norge undertegnet en intensjonsavtale (Memorandum of Understanding) som tar sikte på innføring av «eCall», og EU-kommisjonen er etter det Personvernkommisjonen erfarer i forhandlinger med bilprodusenter om montering av GPS-enheter. En prosjektgruppe (med deltagelse fra Datatilsynet) arbeider med hvordan en slik ordning kan implementeres i Norge. Datatilsynet sammen med Artikkel 29 arbeidsgruppen anerkjenner at formålet bak «eCall» er godt, men påpeker samtidig at systemet reiser flere problemer med hensyn til personopplysningsvern (jf. Art 29 WP 2006b). De mener i hovedsak at den enkelte selv må kunne bestemme om «eCall»-boksen skal være aktivert eller ikke.

Automatisk trafikk-kontroll (ATK) – og kanskje særlig streknings-ATK (måling av gjennomsnittsfart) – er et viktig virkemiddel for å forebygge/unngå ulykker. ATK har til nå vært basert på fartsmåling på ett punkt. Da er det bare de som bryter fartsgrensen ved det aktuelle punkt som blir fotografert. Imidlertid forberedes det nå inn-

føring av streknings-ATK, der det vil bli tatt bilde av alle biler mellom kamera A og kamera B, også av de som holder fartsgrensen ved første målepunkt. Bildene må ha høy kvalitet slik at bilen sikkert kan identifiseres. Så snart man har passert kamera B slettes bildene for de som overholder fartsgrensen. Videre lagring av dataene gjelder bare de som har kjørt for fort. Det har vært et demonstrasjonsprosjekt for streknings- ATK ved Lillehammer, i forbindelse med «0-visjonsprosjektet» som viste at bildene til de som holdt fartsgrensene ble slettet. Fra 2009 vil dette systemet bli innført på E18 i Bamble og på E6 ved Øyer. Etter at systemet har vært i bruk en tid vil det bli evaluert før det eventuelt installeres andre steder i landet. Det eksisterer fortsatt utfordringer her, bl.a. i forbindelse med oversendelse av data til politiet.

17.4 Bekjempelse av kriminalitet og terror

17.4.1 Transportsektoren

Transportsektoren er sterkt preget av en økning i overvåknings- og andre kontrolltiltak som har til formål å sikre storsamfunnet mot kriminelle handlinger. Dette skyldes langt på vei terroristhandlingene i USA 2001, samt bombeangrepene i Madrid 2004 og London 2005. Økningen i slike sikkerhetstiltak har imidlertid ikke vært uniform over hele transportsektoren. Den har vært særlig markant innenfor luftfart og sjøfart, og mindre markant innenfor andre transportgrener som jernbane og veitransport (jf. Bjørnskau et al. 2007).

Innen sjøfart har identifikasjonsbevis for sjøfolk blitt strengere. Det samme har krav til sikkerhet og terrorberedskap for skip og havneområder (se videre Bjørnskau et al. 2007).

Når det gjelder luftfart har security-sjekk av flymannskap, flypassasjerer og deres bagasje blitt intensivert de siste årene. Krav til identifikasjonsbevis for flypassasjerer er blitt strengere, med bl.a. innføring av nye pass med flere biometriske data enn tidligere. Fingeravtrykklesere er dessuten tatt i bruk for å kontrollere forbindelsen mellom innsjekket bagasje og flypassasjerer. Passasjerers bruk av fingeravtrykkleserne ved norske flyplasser er imidlertid valgfritt – etter påtrykk fra Datatilsynet. Men generelt sett er biometriske identifikasjons- og verifikasjonssystemer på vei inn i full fart i en rekke ulike sammenhenger, også utenfor samferdselssektoren, jf. bl.a. Economist (2003) og Scientific American (2008).

Et security-tiltak ved flyplasser som har vakt særlig oppsikt er kroppsskanning. Utstyr for kroppsskanning gjør det mulig å gjennomlyse klær slik at kroppens konturer og gjenstander skjult under klærne blir synlige for kontrollørene. Slikt utstyr er tatt i bruk bl.a. i Schiphol flyplass ved Amsterdam. Dessuten har Europa-kommisjonen nylig fremmet et utkast til forordning som åpner for bruk av kroppsskanning ved europeiske flyplasser (jf. Draft Commission Regulation supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No. 300/2008). Utkastet til forordningen tillater kroppsskanning «individually or in combination, as a primary or secondary means and under defined conditions», men gjør den ikke nødvendigvis obligatorisk.

Europaparlamentet har vedtatt en resolusjon den 23. oktober 2008 som er sterkt kritisk til kommisjonens forslag og uttrykker tvil om dets forholdsmessighet (Europa-parlamentet 2008). Resolusjonen omtaler kroppsskanning som «equivalent to a virtual strip search». Den hevder videre at kroppsskanning er

> "far from being merely technical [but] has a serious impact on the right to privacy, the right to data protection and the right to personal dignity, and therefore needs to be accompanied by strong and adequate safeguards."

Parlamentet er særlig kritisk til at kommisjonen har fremmet forordningsutkastet uten å ha foretatt systematiske konsekvensutredninger inklusiv en «impact assessment relating to fundamental rights». Parlamentet oppfordrer kommisjonen til å foreta en slik undersøkelse samt «scientific and medical assessment of the possible health impact of such technologies» og en «economic, commercial and cost-benefit impact assessment». Som følge av parlamentets resolusjon har kommisjonen nylig utsatt skanningsplanene (jf. The Age 2008).

Avinor planla å teste ut kroppsskannere på Sola flyplass i løpet av våren 2008, men dette er blitt utsatt på ubestemt tid på grunn av sterk motstand fra publikum og Datatilsynet (jf. Aftenposten 2007). Dersom Avinor skulle ønske å teste slikt utstyr, måtte det søkes om samtykke fra Luftfartstilsynet og Samferdselsdepartementet. Søknaden måtte inneholde en beskrivelse av formålet med skanningen, hvor utstyret tenktes brukt, hvordan security-nivået skulle opprettholdes, beskrivelse av ivaretakelse av hms-krav overfor ansatte og passasjerer/ansatte, etc. Hvis Luftfartstilsynet/Samferdselsdepartementet hadde samtyk-

ket i en slik søknad/prosjekt, ville denne måtte fremsendes til EU som også måtte gi sin tilslutning. EU har samtykket til slike tester bl.a. i Sverige, Finland, England, Frankrike og Nederland. Godkjennelsene er gitt under forutsetning av at det å gå igjennom en kroppsskannemaskin skal være frivillig og at passasjerer/ansatte følgelig kan velge å gå igjennom konvensjonell sikkerhetskontroll hvis de heller ønsker det.

Når det gjelder security-tiltak innen andre transportgrener, er det særlig tiltakende videoovervåkning på buss, tog og i drosjer som har vakt debatt i forhold til personvernet. Det har i den senere tid kommet ønsker fra NSB, AS Sporveisbussene og enkelte andre busselskaper om videoovervåkning av deres tog og busser. Datatilsynet godtok i første omgang overvåkningen av inngangsparti og førerkabin i tog og busser, men ikke av passasjerkupeene. Etter klage til Personvernnemnda ble det åpnet for overvåkningen også av kupeene, men under nærmere gitte vilkår (se videre avsnitt 17.4.8 nedenfor).

NSB har fått godkjenning for et prøveprosjekt med å installere videokamera på togtype 69 C (eldre lokaltog). Planen er å installere slike kameraer i andre togtyper senere. NSB har en avtale om at videokameraer skal monteres i alle nye tog som leveres etter 2011. Behovet for slike tiltak er begrunnet i å verne de ansatte og passasjerer, særlig i forhold til ran og overfall. I tillegg er forebygging av hærverk holdt fram som en faktor.

I minst ett tilfelle har denne type overvåkning hatt påvisbar nytte for fremskaffelse av bevis i forhold til overfall (jf. VGnett 2005). Videre viser empiriske undersøkelser at folk flest ser ut til å være positive til denne type overvåkning (jf. bl.a. Transportbedriftenes Landsforening 2005).

17.4.2 Kommunikasjonssektoren

Vi ser stadig mer omfattende overvåkning, registrering, behandling og tapping av kommunikasjon, særlig elektronisk kommunikasjon over Internett. Dette er eksemplifisert ved den såkalte «FRA-loven» som har blitt vedtatt i Sverige, og som gir Försvarets radioanstalt (FRA) adgang til å overvåke all kabelbåret teletrafikk som krysser Sveriges grenser fra den 1. januar 2009 (jf. kapittel 4.4.1). Sverige synes å være blant ytterst få land som har forankret et system for vidtfavnende overvåkning av elektronisk kommunikasjon i formell lov. Det betyr imidlertid ikke at Sverige er alene om å etablere et slikt system. I USA opererer Federal Bureau of Investigation og National Security Agency et lignende system som heter «DCS» («Digital Collection System», tidligere kalt «Carnivore», jf. bl.a. Wall Street Journal (2008). Et omfattende overvåkningssystem som går under navnet «Echelon» påstås også å være etablert av USA med hjelp av enkelte allierte (jf. kapittel 4.4.1), men dets eksistens er aldri blitt offisielt bekreftet av amerikanske myndigheter.

Økende digitalisering av informasjon og billigere datakraft vil gjøre det lettere for flere aktører å igangsette omfattende overvåkning av elektronisk kommunikasjon.

Systematisk overvåkning av nettkommunikasjon skjer også i privat regi. Slik overvåkning skjer utover det å sikre vitale nasjonale sikkerhetsinteresser (herunder rikets sikkerhet). I Norge har for eksempel Simonsen advokatfirma DA fått i oppdrag av platebransjeorganisasjonen IFPI (International Federation of the Phonographic Industry) og filmindustrien (Motion Picture Association) å overvåke nettbruk. Formålet er bekjempelse av ulovlig nedlastning og deling av opphavsrettsbeskyttet materiale på Internett. Simonsen har fått konsesjon fra Datatilsynet til å registrere og viderebehandle IP-adresser som kan benyttes for dokumentasjon ved anmeldelser til politiet. Etter dagens lovgivning (jf. 17.4.3 nedenfor) har imidlertid Simonsen og andre private parter ikke adgang til å spore en IP-adresse til en spesifikk abonnent, dersom abonnenten er en person med dynamisk IP-adresse.

Nye regimer for obligatorisk lagring av trafikkdata utgjør en annen utfordring for personvernet i forhold til elektronisk kommunikasjon. Fremveksten av slike regimer er blitt påskyndet av direktiv 2006/24/EF (datalagringsdirektivet), som tar sikte på å skape et felles regelverk på europeisk nivå for lagring av trafikkdata generert ved bruk av offentlig tilgjengelige elektroniske kommunikasjonsnettverk og -tjenester. Hvorvidt og hvordan direktivet skal implementeres i Norge, er per i dag fremdeles usikkert; hvorvidt direktivet er EØS-relevant likeså. Direktivet har imidlertid vært gjenstand for massiv debatt, både her i Norge og i Europa ellers, og har vært den desidert høyest profilerte saken vedrørende personopplysningsvern i perioden Personvernkommisjonen har vært virksom. Det er derfor grunn til å se på direktivet i detalj.

Direktivets overordnete formål er oppklaring av alvorlig kriminalitet (jf. artikkel 1(1)). Begrepet «alvorlig kriminalitet» («grov kriminalitet» i den danske versjonen av direktivteksten; «serious crime» i den engelske versjonen) er ikke definert.

Det følger videre av artikkel 1(1) at det er opp til nasjonale myndigheter å bestemme hva som nærmere skal ligge i begrepet. Som utdypet nedenfor er terskelen for at politiet skal få tilgang til lagrede trafikkdata, etter dagens regelverk i Norge, langt lavere enn hva direktivet legger opp til. Norsk politi kan få tilgang dersom dataene antas å ha betydning som bevis for etterforskning av enhver type kriminalitet, ikke bare grov kriminalitet.

Etter direktivet er det trafikk- og lokasjonsdata som skal lagres, jf. straks nedenfor. I tillegg skal det lagres data som kan koble trafikkdata til abonnenten/brukeren, altså abonnentsdata. Det fremgår klart av direktivet at kommunikasjonsinnhold ikke skal lagres (jf. artikkel 1(2)).

Opplysninger knyttet til fast- og mobiltelefoni skal lagres. Direktivet pålegger også lagring av opplysninger om bruk av Internett og e-post. Artikkel 5 presiserer hva som skal lagres; trafikk- og lokaliseringsdata. Dette omfatter opplysninger som for eksempel abonnentsdata, oppringt telefonnummer, mislykkede forsøk på oppringning, tidspunkt, fra hvilket område, samtalevarighet, på- og avloggings-informasjon, brukernavn og IP-adresser.

Opplysningene skal lagres fra seks måneder til inntil to år (jf. artikkel 6). Innenfor denne rammen er det opp til hvert enkelt land å bestemme lagringsperioden.

Lagringen skal skje hos tilbyderne av offentlig tilgjengelige elektroniske kommunikasjonsnettverk og -tjenester. Hvem som skal ha tilgang til opplysningene er ellers noe uklart i direktivet. Det følger av artikkel 4 at opplysningene kun skal utleveres til «kompetente nasjonale myndigheder».

Direktivet skulle opprinnelig implementeres innen 15. september 2007. De fleste land i EU har implementert eller er i gang med å implementere direktivet. Danmark vedtok allerede i 2002 en lovendring som pålegger teletilbydere å oppbevare trafikkdata i ett år (jf. retsplejeloven § 786 stk. 4). En del EU-medlemsstater (inklusive Sverige) har valgt å utsette implementering av direktivets bestemmelser vedrørende Internett fordi bestemmelsene er for vage og tvetydige. Irland, støttet av Slovakia, har samtidig anlagt sak for å få direktivet kjent ugyldig (jf. sak C-301/06, Irland mot Rådet og Parlamentet). Det er viktig å påpeke at Irland ikke har anlagt sak på grunn av uenighet om de materielle reglene i direktivet (selv om Irland har ønsket å ha lengre lagringstid enn hva direktivet legger opp til). Saken har derimot et rettsteknisk grunnlag; Irland mener direktivets regler burde vært innlemmet i et «tredje søyle»-instrument (vedrørende politisamarbeid og kriminalitetsbekjempelse), ikke et indre marked-direktiv. En general-advokat ved EF-domstolen har 14. oktober 2008 avgitt uttalelse om at direktivet står på riktig juridisk grunnlag. En slik uttalelse er ikke bindende for EF-domstolen, men generelt sett følger ofte domstolen general-advokatens linje. Utfallet av saken vil langt på vei være bestemmende for hvorvidt direktivet kan innlemmes i EØS-avtalen og dermed gjøres bindende for Norge. I Norge utarbeides det imidlertid et forslag til implementering av datalagringsregler uansett sakens utfall. For videre drøftelse av direktivets EØS-relevans, samt mulighetene for Norge til å reservere seg mot implementering av direktivet, se Arnesen og Sejersted (2008).

Hovedbegrunnelsen for direktivet er å sikre at elektroniske spor som kan ha betydning for oppklaring og bekjempelse av alvorlig kriminalitet blir liggende tilgjengelig for politiet i en viss periode etter at teletilbydere og ISPer ikke lenger trenger å lagre sporene for fakturering og tilrettelegging av kommunikasjon. Lagring av en del abonnentopplysninger, inklusive trafikkdata, er nå tillatt i 3–5 måneder, basert på teletilbyderens fakturerings- og kommunikasjonsbehov. Politiet har anledning til å få utlevert disse opplysninger, eksempelvis for å kunne knytte en IP-adresse til en spesifikk abonnent.

For internettrafikk (IP-aksess og e-post) vil det ikke skje noen endring. Disse tjenestene har hele tiden har vært solgt med forskuddsfakturering for tilgang. Men for fast- og mobiltelefoni er teletilbydernes faktureringsrutiner under endring som følge av den teknologiske utviklingen. Det forventes at tilbyderne vil gå bort fra å fakturere for bruk av tjenester og over til å fakturere for tilgang til tjenestene. For fakturering for tilgang (forskuddsfakturering) er det ikke nødvendig å lagre trafikkdata. Da er tilbyderne etter dagens regelverk forpliktet til å slette de dataene som ikke kan lagres med hjemmel i tilbyderens kommunikasjonsbehov. Politiet hevder at de derved vil miste tilgang til informasjon som kan være verdifull for etterforskning og straffesaksbehandling i retten, ikke bare for å peke ut en skyldig, men også for å utelukke uskyldige (Fløisbonn 2008).

Det er imidlertid uttrykt tvil om lagringsplikten er i samsvar med EMK artikkel 8, særlig kravet til proporsjonalitet (jf. eksempelvis Art 29 WP 2005b). Noen sår også tvil om implementering av direktivet virkelig vil kunne redusere risikoen for alvorlig kriminalitet og terror, samt øke muligheten for å opp-

klare slikt (jf. eksempelvis Jarbekk 2008). Enkelte beskriver videre direktivet som et paradigmeskifte der prinsippet om at politiets virkemidler skal rettes mot en bestemt gruppe blir fraviket og uskyldspresumpsjonen dermed snudd – med andre ord: «Hele folket blir satt under mistanke» (jf. Slettemark 2006). Det er dessuten hevdet at datalagringen som følger av direktivet kan få en dempende effekt («chilling effect») på ytringsfriheten. I denne sammenheng fremheves det at datalagringen vil redusere mulighetene for anonym kommunikasjon og at mange institusjoner/personer – krisesentre, hjelpetelefoner, forsvarere og lignende – er avhengig av slike muligheter. Det fremheves videre at pressens frihet og kildevernet blir satt under press, da det bl.a. vil bli vanskeligere for pressen å beskytte sine kilder (jf. Omdahl 2008).

Bekymringer vedrørende sikkerheten for de lagrede dataene er også blitt luftet. Mange har fremhevet det som en trussel at et stort antall teletilbydere og ISPer pålegges å lagre en svært stor mengde opplysninger på vegne av myndighetene. Det påstås at teletilbyderne ikke vil ha noen egeninteresse i å lagre opplysningene utover egne fakturerings- og markedsmessige formål, noe som vil kunne gå ut over opplysningenes sikkerhet. Samtidig vises det til en rekke episoder fra nyere tid der organisasjoner i både privat og offentlig sektor har latt store mengder personopplysninger komme på avveie.

Et annet sett med bekymringer knytter seg til formålsutglidning. Det påstås at dataene som blir lagret, vil representere en nesten uimotståelig fristelse for ulike aktører i samfunnet å benytte seg av og til en rekke forskjellige formål (jf. eksemplevis Jarbekk 2008).

Personvernkommisjonen har i juni 2008 avgitt en uttalelse om datalagringsdirektivet (se vedlegg 1) som tar opp en del av disse problemstillingene.

17.4.3 Rettslig regulering på området

Samferdselssektoren er stor og mangeartet; angjeldende regelverk er likedan. Her er det mange aktører, enda flere regler, unntakshjemler og til dels motstridende regelverk. Det fastsettes både regelverk som skal sikre personvernet og regelverk som må ses på som klare innskrenkinger av personvernet. Det siste gjelder særlig regelverk for å bekjempe alvorlig kriminalitet. Det juridiske landskapet er med andre ord krevende på flere måter.

En fyldig redegjørelse for den personvernrelevante rettslige reguleringen innen samferdselsområdet ville kreve flere sider enn hele denne rapporten. Det er følgelig ikke anledning her til å presentere dette regelverket i detalj. Regelverket vedrørende transportsektoren er i en særstilling hva gjelder størrelse, kompleksitet og «tetthet». Deler av dette regelverket er dessuten vanskelig tilgjengelig, ikke bare på grunn av komplekst innhold, men også fordi det er unntatt offentlighet. Dette gjelder deler av EUs forordning 622/2003 om foranstaltninger til gjennomføring av grunnleggende felles normer for luftfartssikkerhet. For en grundig gjennomgang av personvernrelevante bestemmelser i lovgivning mv. vedrørende luftfart og jernbane, se Schartum (2007) kapittel 16.

I dette avsnittet presenteres det regelverk som primært gjelder kommunikasjonsvern. Det rettes særlig oppmerksomhet mot elektronisk kommunikasjon. Også enkelte rettslige problemstillinger i forhold til overvåkning av visse former for transport og ferdsel blir presentert.

17.4.4 Kommunikasjonsvern etter EMK

Kommunikasjon er uttrykkelig vernet etter EMK artikkel 8(1), som refererer til retten til respekt for «korrespondanse» i tillegg til privatliv mv. Begrepet «korrespondanse» tolkes på romslig vis, slik at det omfatter et bredt spekter av kommunikasjonsformer, fra bl.a. papirbrev til telefoni til e-post, jf. for eksempel EMDs avgjørelser i *Golder mot Storbritannia* (dom 1975-02-21) (papirbrev), *Malone mot Storbritannia* (dom 1984-08-02) (telefoni) og *Copland mot Storbritannia* (dom 2007-04-03) (e-post og bruk av Internett). Disse sakene er nærmere beskrevet i andre deler av rapporten samt i vedlegget om grunnlovsfesting av retten til personvern/privatliv. EMDs praksis viser samtidig at kommunikasjon (i hvert fall mellom privatpersoner) også nyter vern som del av de øvrige elementer i artikkel 8(1), særlig privatliv («private life»).

Avlytting eller opptak av telefonsamtaler mv. uten at de kommuniserende personene har avgitt samtykke til eller blitt informert om dette, og der disse har en rimelig forventning om at samtalen er privat, utgjør et inngrep i rettigheten(e) etter artikkel 8(1). Dette gjelder uansett om kommunikasjonen skjer innenfor det private hjem eller utenfor – eksempelvis på en arbeidsplass (jf. bl.a. *Halford mot Storbritanni*a (dom 1997-06-25)).

Teletilbyderes utlevering av trafikkdata til politiet vil også kunne utgjøre et inngrep i samme rettigheten(e) (jf. Malone-saken referert ovenfor).

Alle slike inngrep må rettferdiggjøres i henhold til de kriteriene artikkel 8(2) oppstiller. Det

vil si at de må ha klar lovhjemmel og være nødvendige i et demokratisk samfunn for å ivareta visse samfunnsinteresser (jf. kapittel 6.1.3). Mesteparten av EMDs praksis vedrørende kommunikasjonsvern dreier seg om avlytting og lignende former for kommunikasjonskontroll foretatt av politiet. I de fleste saker har EMD funnet at EMK artikkel 8 er blitt krenket fordi den angjeldende kommunikasjonskontrollen har manglet klar lovhjemmel (jf. eksempelvis Malone, Halford og Copland-sakene, jf. også *Kruslin mot Frankrike* (dom 1990-04-24), *Huvig mot Frankrike* (dom 1990-04-24) og *Khan mot Storbritannia* (dom 2000-05-12). Disse sakene dreier seg stort sett om engelsk og fransk regelverk om kommunikasjonskontroll. EMD har aldri blitt forelagt norsk regelverk på området for vurdering.

17.4.5 Vern mot overvåkning av offentlig ferdsel etter EMK

EMK artikkel 8 gir et visst vern mot overvåkning av ferdsel (og annen menneskelig aktivitet) som skjer ute i det offentlige rom. Dette er eksemplifisert i Peck- og von Hannover-sakene (begge omtalt i kapittel 13.2.2). Det er imidlertid viktig å merke seg to forhold som begrenser dette vernet. For det første har EMD ikke uttrykkelig anerkjent en rett til anonym ferdsel i det offentlige rom som del av rettighetskatalogen i artikkel 8(1). Det andre er at EMD i utgangspunktet ikke anser observasjon av personer, med mindre det skjer et forholdsvis varig maskinelt opptak av det som blir observert, som et inngrep i rettigheten(e) etter artikkel 8(1). Som domstolen fastholder i *P.G. og J.H. mot Storbritannia* (dom 2001-09-25) (avsnitt 57):

> "There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain."

Det er med andre ord først når det skjer systematisk eller varig opptak av personlig aktivitet ute i det offentlige rom at elementene i artikkel 8(1) får relevans. Dette bekreftes bl.a. i saken *Perry mot Storbritannia* (dom 2003-07-17) der EMD uttaler (jf. avsnitt 38 og 40):

> "The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life.
>
> [T]he normal use of security cameras per se whether in the public street or on premises, such as shopping centres or police stations where they serve a legitimate and foreseeable purpose, do not raise issues under Article 8 § 1 of the Convention."

Uttalelsen synes å forutsette at fjernsynsovervåkningen er åpenbar for de som blir observert. Uttalelsen synes dessuten å forutsette at fjernsynsovervåkningen tjener et legitimt og påregnelig formål. Den tar imidlertid ikke direkte stilling til hvorvidt hemmelig fjernsynsovervåkning, uten varig/systematisk opptak, men til formål som er legitime og påregnelige, også faller utenfor artikkel 8(1). Av andre avgjørelser som ikke omhandler grensene for fjernsynsovervåkning fremgår det at hemmelig registrering av personopplysninger, selv til legitime formål (som kriminalitetsbekjempelse), vil kunne utgjøre et inngrep i rettigheten(e) etter artikkel 8(1) (jf. bl.a. *Leander mot Sverige* (dom 1987-3-26).

Det at domstolen langt på vei lar åpen fjernsynsovervåkning faller utenfor anvendelsesområdet for artikkel 8 er blitt kritisert (jf. Sunde 2008, Lomell 2005). Sunde skriver for eksempel:

> «Et spørsmål er om man uten videre bør godta likestillingen av en vaktmanns observasjoner via kamera, med observasjoner gjort av personer som selv er fysisk tilstede. Det kan hevdes at man er i det offentlige rom overfor personer som selv gir seg tilkjenne, mens man har rett til å holde på sin privatsfære overfor anonyme observatører. Bør ikke selve disiplineringseffekten av å vite seg observert, uten at man vet av hvem, anses som et inngrep i privatlivet?»

Hun påpeker videre at EMDs tilnærming ikke tar tilstrekkelig høyde for en situasjon med svært omfattende fjernsynsovervåkning. Vi kommer tilba-

ke til denne kritikken i avsnittene 17.4.8 og 17.5 nedenfor.

17.4.6 Kommunikasjonsvern etter norsk rett

Sentrale bestemmelser om vern av kommunikasjon generelt finnes i straffeloven, særlig § 145 første ledd («brevbruddsbestemmelsen» som beskytter «lukket skrift» og lignende kommunikasjonsformer), § 145 andre ledd (som straffer uberettiget tilgang bl.a. til «data», inklusiv personopplysninger) og § 145a (som straffer uberettiget avlytting og opptak av samtaler og forhandlinger).

Når det gjelder vern av elektronisk kommunikasjon, finnes det også viktige bestemmelser i lov om elektronisk kommunikasjon (ekomloven), som blant annet gjennomfører direktiv 2002/58/EF om elektronisk kommunikasjon og personvern (kommunikasjonsverndirektivet). Lovens § 2-9 pålegger tilbydere av teletjenester mv. taushet om innholdet av elektronisk kommunikasjon og andres bruk av denne kommunikasjon. Taushetsplikten «er ikke til hinder for at det gis opplysninger til påtalemyndigheten eller politiet om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse», jf. § 2-9 tredje ledd. Anmodning om slike opplysninger skal etterkommes «med mindre særlige forhold gjør det utilrådelig», jf. fjerde ledd. Teletilbyderne er videre forpliktet til å «tilrettelegge nett og tjeneste slik at lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon sikres», jf. § 2-8. Politiet må imidlertid gi en teletilbyder tilstrekkelig entydige opplysninger om abonnenten til at teletilbyderen relativt lett kan utlevere de nevnte opplysningene. Dette følger av Høyesteretts kjennelse i Rt. 1999, s. 1944 og er grunnet i personvernhensyn.

Teletilbydere er dessuten forpliktet til å registrere identifikasjonsopplysninger om abonnenter – inklusive ved utstedelse av kontantkort for mobiltelefoni, jf. ekomforskriften § 6-2. Dette medfører reduserte muligheter for anonym telekommunikasjon.

Reglene om teletilbyderes ansvar for overføring og lagring av data med ulovlig innhold fastholder likevel at teletilbyderne ikke har en generell plikt til å overvåke den informasjon de overfører eller lagrer. De har heller ingen generell plikt til aktivt å søke etter fakta eller forhold som indikerer ulovlig aktivitet. Dette følger av ehandelsloven § 19 som implementerer ehandelsdirektivet (2000/31/EF) artikkel 15.

Når det gjelder teletilbydernes lagring av trafikkdata, skal slike data «slettes eller anonymiseres så snart de ikke lenger er nødvendig for kommunikasjons- eller faktureringsformål, med mindre annet er bestemt i eller i medhold av lov» eller det foreligger samtykke fra abonnenten/brukeren (jf. ekomloven § 2-7 annet ledd).

Trafikkdata er ansett som personopplysninger etter personopplysningsloven. Lagring og behandling av slike opplysninger for faktureringsformål og administrasjon av kundeforholdet reguleres dermed av personopplysningsloven. Teleoperatørenes behandling av trafikkdata er konsesjonspliktig, jf. personopplysningsloven §§ 33–34 og personopplysningsforskriften § 7-1. De nærmere vilkårene for lagring, bruk og sletting følger av konsesjonsvilkårene. Det normale er at opplysninger kan lagres til fakturaen er betalt, som regel en periode på tre til fem måneder. Se videre Datatilsynets standardkonsesjon for teletilbydere pkt. 8.[1]

Politiets adgang til å foreta kommunikasjonskontroll og innhente trafikkdata er i hovedsak hjemlet i straffeprosessloven kapitler 16 – 16b. Dette gjelder både avlytting og opptak av sanntidskommunikasjon, tilgang til trafikkdata i sanntid, samt tilgang til allerede lagrede trafikkdata (ofte kalt «historiske» trafikkdata). Hovedregelen er at retten kan tillate politiet å foreta avlytting/opptak av sanntidskommunikasjon når det er skjellig grunn til mistanke om en forbrytelse der strafferammen er 10 år eller mer, eller det foreligger skjellig grunn til mistanke om visse andre grove forbrytelser som er konkret angitt i loven, jf. § 216a første ledd. Terskelen for tilgang til sanntidstrafikkdata er lavere: Her må det i hovedsak foreligge skjellig grunn til mistanke om en forbrytelse som kan medføre fengsel i 5 år eller mer, jf. § 216b første ledd, jf. § 216b annet ledd, bokstav d). Skjellig grunn til mistanke om visse andre angitte straffbare handlinger – som brudd på straffeloven § 145 andre ledd («datainnbrudd», se ovenfor) eller straffeloven § 390a (skremmende eller plagsom opptreden) – er også tilstrekkelig. Når det gjelder tilgang til lagrede eller historiske trafikkdata, er terskelen enda lavere. Politiet kan få dataene utlevert i medhold av straffeprosessloven § 210, så fremt disse «antas å ha betydning som bevis» (jf. Rt. 1992, s. 904, Rt. 1997, s. 470).

For avlytting og opptak av kommunikasjon, samt tilgang til sanntidstrafikkdata må kontrollen

[1] Tilgjengelig ved http://www.datatilsynet.no/upload/Dokumenter/konsesjoner/konsesjon_tele_m_merkn.pdf (sist besøkt 12.11.2008).

antas å være av vesentlig betydning for å oppklare saken og at oppklaring i vesentlig grad vil bli vanskeliggjort dersom denne kontrollen ikke skjer, jf. straffeprosessloven § 216c. I tilfeller der den aktuelle personen eller datamaskinen som ønskes avlyttet må antas å bli brukt av et større antall personer, må det i tillegg foreligge «særlige grunner» for å foreta avlyttingen. Dette gjelder også i forhold til kontroll av kommunikasjon mellom mistenkte og dennes advokat, lege, prest eller andre som erfaringsmessig fører samtaler av svært fortrolig art (med mindre den mistenkte selv er vedkommende advokat, lege mv.), jf. § 216c annet ledd.

Som «tvangsmiddel» er bruk av kommunikasjonskontroll dessuten underlagt generelle krav etter § 170a. Kontrollen må være tilstrekkelig grunnet og må ikke anses uforholdsmessig.

Det er retten som avgjør om kommunikasjonskontroll kan skje, jf. straffeprosessloven §§ 216a og 216b første ledd, jf. § 216e første ledd. Dersom det ved opphold er stor fare for at etterforskningen vil lide, kan påtalemyndigheten beslutte igangsetting av kommunikasjonskontroll, jf. § 216d første ledd. I så fall skal denne beslutningen snarest mulig og senest innen 24 timer etter oppstart av kontrollen forelegges retten for godkjennelse.

Det er satt begrensninger på hvor lenge slik kommunikasjonskontroll kan vare. Som hovedregel skal slik kontroll ikke vare lenger enn «strengt nødvendig», og ikke mer enn 4 uker ad gangen, jf. § 216f. Opptak mv. som slik kontroll genererer, skal slettes dersom de ikke har betydning for å forebygge eller etterforske straffbare forhold, jf. § 216g.

17.4.7 Regler for bruk av kryptografi

Et viktig teknologisk middel for å sikre kommunikasjonsvern er bruk av kryptografi. Det finnes imidlertid forholdsvis få rettsregler i norsk rett som direkte omhandler bruk av kryptografi. Rettslige restriksjoner på import og bruk av kryptografi i Norge finnes ikke. Derimot finnes det rettslige krav til bruk av kryptografi av en viss styrke på bestemte områder, for eksempel ved elektronisk formidling av taushetsbelagte opplysninger til forvaltningsorganer (jf. forskrift om elektronisk kommunikasjon med og i forvaltningen 28. juni 2002 nr. 656, §§ 20–23), ekstern dataoverføring av sensitive personopplysninger (som definert i personopplysningsloven, jf. personopplysningsloven § 13, jf. personopplysningsforskriften § 2-11 tredje ledd), eller ved behandling av sikkerhetsgradert informasjon (som definert i sikkerhetsloven, jf. lovens § 11). Det finnes i tillegg restriksjoner på eksport av kryptoprodukter til visse land i henhold til eksportkontrolloven og det såkalte Wassenaar-arrangementet. Sistnevnte er et samarbeid mellom en rekke land som regulerer grensekryssende omsetning av våpen og høyteknologiprodukter som kan anvendes som våpen («dual-use» produkter), herunder kryptoprodukter (se videre, Bygrave 2003, s. 267f).

Blant rettsregler som mer indirekte omhandler bruk av kryptografi, er regler som krever eller forutsetter sikring av datakonfidensialitet og -integritet de mest sentrale. Selv om disse reglene ikke nevner bruk av kryptografi, er det innlysende at bruk av kryptografi langt på vei vil kunne oppfylle deres krav. Slike regler går igjen i store deler av regelverket bl.a. i form av taushetspliktsbestemmelser. Bestemmelser i straffeloven om forskjellige typer datakriminalitet vil også kunne bidra til beskyttelse av krypterte data og krypteringsmekanismer. Krav til bruk av kryptografi kan dessuten være avtalebasert.

I tillegg finnes folkerettslige regler som indirekte bidrar til å beskytte bruk av kryptografi . Både EMK artikkel 8 og artikkel 10 kan tenkes å kunne understøtte slik bruk i og med at personvern og ytringsfrihet vil kunne fremmes gjennom tiltak for sikring av kommunikasjonskonfidensialitet.

17.4.8 Personopplysningsloven

Personopplysningsloven vil i utgangspunktet komme til anvendelse både i forhold til kommunikasjon og transport såfremt det behandles personopplysninger (dvs. opplysninger som kan knyttes til en bestemt fysisk person) og den behandlingsansvarlige er etablert i Norge eller behandler opplysningene ved bruk av hjelpemidler lokalisert i Norge, jf. personopplysningsloven § 3.

Reglene i personopplysningsloven er generelle, sektoroverskridende og langt på vei teknologinøytrale. Loven inneholder imidlertid noen regler som spesifikt tar for seg fjernsynsovervåkning (dvs. «vedvarende eller regelmessig gjentatt personovervåkning ved hjelp av fjernbetjent eller automatisk virkende fjernsynskamera, fotografiapparat eller lignende apparat», jf. personopplysningsloven § 36). Disse reglene er samlet i lovens kapittel VII. Reglene nedfeller krav om når fjernsynsovervåkning kan finne sted, krav til varsling av slik overvåkning og krav vedrørende utleve-

ring av tilhørende billedopptak. I tillegg inneholder kapittel 8 i forskriften til personopplysningsloven enkelte særbestemmelser om fjernsynsovervåkning som bl.a. gjør presiseringer av politiets bruk av opptak, og krav om sletting og rett til innsyn.

Reglene om fjernsynsovervåkning er høyst relevante for person(opplysnings)vernet i forbindelse med transport/ferdsel. Grunnkravet er at fjernsynsovervåkning av steder der en begrenset krets av personer ferdes jevnlig, kun er tillatt dersom det foreligger et særskilt behov for overvåkningen, jf. § 38. Grunnkrav for når overvåkning av offentlige steder kan finne sted følger derimot av vilkår etter § 8. I tillegg skal all fjernsynsovervåkning (også på offentlig sted) varsles, jf. § 40. Når fjernsynsovervåkningen medfører lagring av billedopptak slik at opplysninger om bestemte personer kan gjenfinnes, gjelder hele loven, jf. § 37 annet ledd. Det betyr at reglene om meldeplikt og konsesjonsplikt etter §§ 32 og 33 kommer til anvendelse. Reglene om konsesjonsplikt kommer likevel ikke til anvendelse dersom overvåkningen har til formål å avdekke kriminell adferd, jf. § 2 nr. 8 bokstav b.

Personvernnemnda har behandlet flere klagesaker der fjernsynsovervåkning har vært i fokus. To av disse sakene omhandler transportsektoren.

Klagesak 2005-13: NSB påklagde Datatilsynets vedtak om å begrense videoovervåkning av publikumsområder på lokaltogene til inngangsparti samt togførerkabin. Personvernnemnda kom til at videoovervåkning også inne i kupeene kan tillates. Saken ble avgjort i hovedsak etter en interesseavveining i henhold til personopplysningsloven § 8 bokstav f. Nemnda mente at ulempene for personvernet ved slik overvåkning er beskjedne siden opptakene bare vil bli avspilt og brukt når det skjer en straffbar hendelse på toget. Avspilling vil dessuten skje i henhold til særskilte prosedyrer. Men siden bildene kan inneholde sensitive personopplysninger mente nemnda at overvåkningen og avspilling krever konsesjon. Nemnda fant imidlertid at vilkårene for å utstede konsesjon er til stede.

Klagesak 2005-12: Denne saken gjaldt også adgang til videoovervåkning, men i Sporveisbussenes passasjerkupeer. Klagen ble avgjort på samme måte og grunnlag som for klagesak 2005-13.

Det finnes to andre klagesaker som også er direkte relevante for person(opplysnings)vernet i forbindelse med transport/ferdsel. Disse omhandler ikke fjernsynsovervåkning, men andre former for registrering av ferdsel. Én av sakene (sak 2005-11 omtalt straks nedenfor) er prinsipielt viktig fordi den berører en påstått rett til å kunne ferdes anonymt.

Klagesak 2005-11: Saken omhandler hvorvidt det skal registreres opplysninger om bilister og deres kjøretøy ved passering av helautomatiske bomstasjoner. Da Datatilsynet først utstedte konsesjon for drift av helautomatiske bomstasjoner, ble det satt som vilkår at et anonymt passeringsalternativ skulle være på plass før bomstasjonene ble satt i drift. Statens vegvesen var uenig i Datatilsynets vurdering av hva som er et hensiktsmessig passeringsalternativ. Datatilsynet gikk inn for en løsning som ville beskytte bilisters anonymitet bedre enn løsningen som ble foretrukket av Statens vegvesen. Sistnevntes ønske om ikke å etablere løsningen som Datatilsynet fremmet, var basert på praktiske forhold vedrørende behandling og salg av anonyme brikker (såkalte «ihendehaverbrikker»). Datatilsynet la derimot til grunn at individer har en grunnleggende rett til anonym ferdsel utledet av EMK artikkel 8, SP artikkel 17 og fortalen til EUs direktiv om personopplysningsvern, og at selv om denne retten ikke er absolutt, veier den i utgangspunktet tyngre enn rent kommersielle hensyn.

Personvernnemnda tok ikke direkte stilling til Datatilsynets standpunkt om en påstått rett til anonym ferdsel, men uttalte følgende:

> «[S]pørsmålet om retten til å ferdes anonymt på offentlig sted, og ellers til å opptre anonymt i samfunnet, er et grunnleggende rettspolitisk spørsmål av sentral betydning for personvernet. Det er også et spørsmål som er sektorovergripende. Det fremstår som sterkt ønskelig at man kunne ta stilling til dette spørsmålet generelt, og ikke bare f.eks. i forbindelse med bomsystemer. Personvernnemnda er imidlertid henvist til å begrense sin saksbehandling til en vurdering av den aktuelle klage. Nemnda vil ikke unnlate å bemerke at den oppsplitting i konkrete klager som er nødvendig for prøving av enkeltvedtak ikke må få lov til å erstatte en mer prinsipiell rettspolitisk debatt av den karakter Datatilsynet søker å vekke ved de prinsipielle merknadene til denne saken.»

Personvernnemnda ga likevel Statens vegvesen medhold i sin klage fordi den anonyme løsningen foretrukket av Datatilsynet ville medføre praktiske og kommersielle ulemper som i praksis ikke fremmet personvernet merkbart bedre enn løsningen foretrukket av klageren:

> «I seg selv er disse ulempene på ingen måte avgjørende. Men hvis man skal pålegge behand-

lingsansvarlig slike merkostnader, bør de føre til et bedret personvern for den registrerte.»

Forutsetningen for Personvernnemndas avgjørelse var at registrerte opplysninger ville behandles i tråd med de øvrige konsesjonsvilkårene fastsatt av Datatilsynet, samt at vegvesenets «sporfrie alternativet promoveres, og forholdene legges til rette for at den enkelte kan benytte dette uten at det skal representere praktiske eller økonomiske belastninger».

Den andre klagesaken som er direkte relevant for transportsektoren er følgende:

Klagesak 2007-04: Rogaland Kollektivtrafikk FKF påklagde Datatilsynets vedtak om etablering av Kolumbuskortet, som er et elektronisk reisekort der passasjeren har en Internettbasert «reisekonto» med lagret reisemønster. Klagen gjaldt hvorvidt det forelå en tilstrekkelig dokumentert risikovurdering av dette systemet som var i samsvar med krav etter personopplysningsforskriften kapittel 2. Både Datatilsynet og nemnda konkluderte med at en slik risikovurdering manglet og at tilsynet dermed behøvde ikke å ta stilling til om selve systemet tilfredsstiller personopplysningsloven og forskriften. Selv om saken omhandlet et proseduralt forhold, viser den at også sikkerhetsmessige krav er et viktig vurderingstema i forhold til tiltak som implementeres i samferdselssektoren.

17.5 Personvernkommisjonens observasjoner

Kommisjonens observasjoner er basert på en gjennomgang av relevant dokumentasjon supplert med innspill fra deltagere på et åpent seminar som kommisjonen arrangerte den 10. juni 2008.[2] I tillegg kommer kommisjonens interne ekspertise.

Innen samferdselssektoren finner vi at personvernutfordringer spesielt er knyttet til lagring av trafikkinformasjon (tele, Internett o.l.), betalingssystemer som krever registrering av trafikkadferd (elektroniske systemer for betaling i veitransport, elektronisk billettering i kollektivtrafikk), trygghet (automatisk trafikk-kontroll, kameraovervåkning i kollektive transportmidler), ny kjøretøyteknologi (systemer som viser posisjonering, «eCall» o.l.). De fleste av disse utfordringene skyldes en kombinasjon av legitime ønsker om å forbedre funksjonaliteten og/eller sikkerheten ved samferdsel, kriminalitetsbekjempelse, samt teknologiske nyvinninger som muliggjør eller synes å kunne muliggjøre oppfyllelse av disse ønskene.

Utfordringene er forsterket fordi mange av de hensynene som er med på å svekke personvern anses av beslutningstakere som svært viktige. Hensyn til liv og helse veier tungt når nye elektroniske løsninger blir valgt i samferdselssektoren. Det samme gjelder hensyn til personers trygghet og kriminalitetsbekjempelse når eksempelvis teletilbydere skal pålegges en tilretteleggingsplikt for kommunikasjonskontroll og utlevering av trafikkdata.

Utfordringene er dessuten forsterket på grunn av visse trekk ved det angjeldende regelverket. Jussen på området – både den som har til hensikt å fremme personvern og den som undergraver personvern – er uoversiktlig, kompleks og åpner for mange tolkningsmuligheter. Det er videre et tankekors at en del av regelverket som potensielt medfører inngrep i personvernet ikke er offentlig, jf. EUs forordning om sikkerhet ved luftfart referert i avsnitt 17.4. Dette er et problem, ikke bare i forhold til personvern, men også i forhold til rettssikkerhet og muligheter for demokratisk styring og kontroll ved regelutvikling.

Utfordringene er også blitt forsterket ved at personvernhensyn tilsynelatende bare i forholdsvis begrenset grad har vært vurdert når nye tiltak har blitt etablert innen samferdselssektoren. Vi finner for eksempel at personvern vies lite plass i Samferdselsdepartementets IKT-strategi «Fra A til B... Bedre, tryggere og mer effektiv transport – med IKT» (Samferdselsdepartementet 2002). Man har derimot primært tenkt seg at økt bruk av IKT innen samferdsel skal bidra til å gi bedre sikkerhet og kapasitetsutnyttelse på sektoren, i tillegg til å øke nytten for brukerne.

En intervjubasert undersøkelse av representanter for en rekke organisasjoner med hovedvirksomhet innen transportsektoren konkluderer at «personvernhensyn ikke er svært høyt oppe på dagsorden i det daglige arbeidet, men samtlige aktører har likevel tenkt gjennom de sidene ved personvernet som oppleves som relevante for egen virksomhet» (Bjørnskau et al. 2007, s. 78).

Eva Hildrum ved Samferdselsdepartementet opplyste på Personvernkommisjonens seminar om personvern og samferdsel at neste Nasjonal Transportplan (NTP) for perioden 2010–19 imidlertid skal inneholde en grundig beskrivelse av grenseflater mellom personvernhensyn og samferdselshensyn. En slik omtale av personvern er

[2] Seminarprogrammet er tilgjengelig ved http://www.personvernkommisjonen.no/sem080610/program.pdf.

nytt i NTP-sammenheng. Stortingsmeldingen om NTP skal legges fram ved årsskiftet 2008/09.

Iverksetting av mange security-tiltak i kjølvannet av «9-11» mv. virker langt på vei å være hendelsesstyrt, uten at det er blitt foretatt grundige nytte-kostnadsvurderinger eller andre systematiske konsekvensutredninger på forhånd. Innføring av væskeforbudet på fly er angitt å være et eksempel i så måte (jf. Bjørnskau et al. 2007, ss. 91-95). Dette skjer til tross for at tiltakene er enormt ressurskrevende. Denne utviklingen synes videre å ha ført til en lite rasjonell balanse i sikring mellom transportgrener. For eksempel er en rekke security-tiltak implementert for luftfart mens forholdsvis få er implementert for jernbanetransport. Det samme har skjedd innenfor enkelte transportgrener. I forbindelse med sjøfart, for eksempel, er det iverksatt tiltak for å sikre havn og skip mot anslag via landeveien, men forholdsvis lite er gjort for sikring mot anslag via sjøveien.

Det synes imidlertid å være noen grenser for hva personer er villig til å godta i form av sikkerhetstiltak som påvirker deres personvern. Det synes å være forholdsvis stor skepsis til innføring av security-teknologier som utfordrer eller antas å utfordre kroppens intimsfære (jf. Teknologirådet 2007b, s. 27). Kroppsskanning er hovedeksempel i den forbindelse. Det er videre forholdsvis stor skepsis til innføring av tiltak som får folk til å føle seg mistenkt og som det er vanskelig å forstå nødvendigheten av. Obligatorisk lagring av trafikkdata i henhold til datalagringsdirektivet er hovedeksempel i denne sammenheng.

Likevel er det liten tvil om at den enkeltes mulighet til å kunne ferdes og kommuniseres relativt anonymt er i ferd med å bli betydelig redusert på grunn av økte muligheter for og krav til ulike former for registrering. Økt registreringsnivå med innsamling av personopplysninger innen stadig nye felter, medfører også en risiko for at opplysningene kan komme på avveie eller misbrukes.

Det er samtidig begrensninger på hvorvidt personvernregelverket kan demme opp for denne utviklingen. Noen av disse begrensningene skyldes manglende oppfølging av regelverket. Noen begrensninger skyldes regelverket selv. Men noen ganger legger også de som har i oppgave å tolke og anvende regelverket begrensninger på reglene som ikke behøver å eksistere. Et eksempel er EMDs tilnærming til åpen fjernsynsovervåkning til bekjempelse av kriminalitet som gjør at EMK artikkel 8 legger få begrensninger på slik overvåkning, i hvert fall når overvåkningen ikke medfører systematisk eller varig billedopptak.

Registreringsmulighetene som teknologisk sett er tilgjengelige i dag synes å være tilnærmet ubegrensete, derfor er det avgjørende at de etiske og moralske problemstillingene som dukker opp i kjølvannet av de nye metodene som tas i bruk blir grundig gjennomgått og evaluert. Hvor langt skal vi gå i å lage og implementere systemer som innebærer mulighet for overvåkning eller kontroll for å oppnå økt sikkerhet og/eller effektivitet – og dermed bedre bruk av samfunnets felles ressurser? Teknologisk er det meste mulig i dag, men hva skjer dersom ulike deler av den sektoriserte forvaltningen hver for seg iverksetter egne løsninger? Resultatet kan da bli at ingen har full oversikt over hvordan data kombineres og gjenbrukes dersom sentrale myndigheter ikke er påpasselige og gir klare retningslinjer.

Personvernets utfordringer innen samferdselssektoren er omfattende ettersom man skal arbeide for best mulig trafikksikkerhet i møte de stadig økende kravene til effektivitet innen transport, og samtidig ta de rette grepene, slik at man kan forebygge kriminalitet og terror. Disse oppgavene representerer en utfordring for både lovverket og for de som skal finne fram til de teknologiske løsningene som skal ivareta disse oppgavene.

17.6 Personvernkommisjonens tilrådninger

I lys av disse observasjoner har Personvernkommisjonen følgende tilrådninger.

Den viktigste av disse er økt vektlegging av kravet til proporsjonalitet ved tiltenkt innføring av personverninngripende tiltak innen kommunikasjon og transport. Dette kravet følger allerede av sentrale deler av personvernregelverket (bl.a. EMK artikkel 8 og personopplysningsloven § 8), men det må vektlegges og synliggjøres bedre. Kravet medfører at det foretas systematiske nytte-kostnadsvurderinger og konsekvensutredninger forut for implementering av personverninngripende tiltak. Det medfører videre at behov for slike tiltak blir dokumentert. Det medfører også at dersom tiltaket blir implementert, skal dette skje på en måte som er minst mulig skånsom for personvernet og at svekkelsen av personvernet følgelig blir forsøkt kompensert gjennom andre krav forankret i personvern og/eller rettsikkerhet (eksempelvis solnedgangsklausuler).

Personvernkommisjonen har i juni 2008 avgitt en uttalelse om datalagringsdirektivet som vektlegger slike krav (jf. vedlegg 1). Vi holder fast ved

denne uttalelsen. Det har ikke skjedd noe i mellomtiden som tilsier en endring i vårt prinsipielle standpunkt til regler for datalagring som vi uttrykker i denne uttalelsen.

Når det gjelder politiets kommunikasjonskontroll mer generelt, avstår Personvernkommisjonen fra tilrådninger om hvordan det nåværende regelverket for slik kontroll kunne endres. Vi ser at regelverket er komplisert og til dels uoversiktlig, samtidig som det er omfattende. Men hele dette regelverket, samt eventuell bruk av nye etterforskningsmetoder, er nå under vurdering av Metodekontrollutvalget som skal levere sin rapport i juli 2009. Det følger av Metodekontrollutvalgets mandat at personvernhensyn skal trekkes inn i vurderingen.

Personvernkommisjonen tilrår videre at det så langt som mulig legges til rette for sporfrie og/eller anonyme løsninger i forhold til betaling og bruk av transporttjenester. Grunnregelen bør være at når en tilbyr et elektronisk billettsystem eller lignende, skal det være mulig å benytte seg av et sporfritt alternativ. I dette ligger det også et krav om at bruken av det sporfrie alternativet ikke skal medføre betydelige merkostnader for sluttbrukeren som ikke reflekterer reelle merkostnader for tjenestetilbyderen (jf. bl.a. Personvernnemndas uttalelse i klagesak 2005-11). Tjenestetilbyderen skal dessuten gjøre informasjon om det sporfrie alternativet lett tilgjengelig – noe som per i dag ikke alltid skjer (jf. observasjonene om mangel på promovering av det sporfrie alternativet ved AutoPASS-systemet i avsnitt 17.2). Det at disse dataene ikke er komplette, bidrar til at det er vanskeligere å benytte AutoPASS-systemet til andre formål enn innkreving av betaling (jf. kapittel 4.4.1 om formålsutglidning).

Personvernkommisjonen betrakter det som positivt at Samferdselsdepartementet i stortingsproposisjonen om «Oslopakke 3» har varslet et interdepartementalt samarbeid om anonymitet i helautomatiske bomstasjoner. Resultatet av dette arbeidet skal foreligge innen utløp av Datatilsynets konsesjonsperiode for Osloringen (årsskiftet 2009/2010).

Personvernkommisjonen mener at det også bør gjøres en systematisk innsats for å synliggjøre overfor befolkningen de nye formene for registrering og regelbaserte systemer som i tiltakende grad integreres i produkter og omgivelser, jf. også Teknologirådet (2007a). En rekke produkter som kan kjøpes i dag kommer med innebygd automatikk (eksempelvis i form av evne til automatisk å logge gjenstandens bruk og dens lokalisering). Man bør lett kunne få nærmere opplysninger om rekkevidden av denne type «intelligens».

Samtidig hefter det usikkerhet til hvordan dagens regelverk regulerer bruken av automatiserte registreringsenheter som er innebygd i produkter mv. Dette gjelder eksempelvis spørsmålet om eierskap og adgang til dataene som er generert av kjøreregistratorene i nye biler (jf. avsnitt 17.3). Personvernkommisjonen tilrår derfor at det blir utredet hvordan nåværende regelverk (inklusiv personopplysningsloven) løser slike spørsmål og hvorvidt regelverket bør endres til bedre å fremme personvernhensyn ved produksjon og bruk av slike data.

Personvernkommisjonen tar samtidig avstand fra innføring av automatiske registreringssystemer i alminnelige produkter (f.eks personbiler) der hensikten med registreringen er å ha en disiplinerende funksjon overfor den som bruker produkter (som bilføreren). Kommisjonen anerkjenner at det kan være behov for slike systemer i visse angitte kontekster (for eksempel for å registrere at yrkessjåfører som driver med langtransport overholder pålagte hviletider), men de bør ikke innføres generelt. Forslaget til adferdsboks som er nevnt i avsnitt 17.3, er et eksempel på et system som vi ikke kan godta (jf. avsnitt 4.4). Kommisjonen vil samtidig oppfordre til større bruk av kontrollsystemer som ikke medfører registrering av personopplysninger. Bruk av alkolås i biler er et eksempel; «grønn bølge» (jf. kapittel 10.1.2) et annet.

Avslutningsvis mener Personvernkommisjonen at norsk kryptopolitikk fremdeles bør innta en liberal holdning. Dette tilsier at staten fremdeles bør ta avstand fra innføring av obligatorisk deponering av nøkler som innehas av privatpersoner og skal brukes til rent personlige formål og/eller kun autentiserings-/signeringsformål. Staten bør videre vise stor forsiktighet ved å innføre andre begrensninger på folks rett til å ta i bruk sterk kryptering (jf. Bygrave 2003).

Del V
Andre områder kommisjonen har arbeidet med

Kapittel 18
Organisering av personvernmyndighetene

18.1 Innledning

I følge mandatet skal Personvernkommisjonen kartlegge og evaluere de virkemidlene som eksisterer for å ta vare på personvernet, herunder se på personvernmyndighetenes praksis og rolle.

En rekke tilsynsmyndigheter i Norge har med behandling av personopplysninger å gjøre. Personopplysningsbegrepet er vidt (jf. avsnitt 4.5.3) og omfatter derfor opplysninger innenfor en rekke sektorer der det kan være myndigheter med særskilt kompetanse. Eksempler på slike er Arbeidstilsynet, Barneombudet, Forbrukerombudet, Kredittilsynet, Post- og teletilsynet, Sivilombudsmannen, Helsetilsynet, regionale komiteer for medisinsk og helsefaglig forskningsetikk, uten at denne listen er uttømmende. Disse myndighetenes virkeområde er imidlertid ikke spesielt knyttet opp til behandling av personopplysninger, selv om slike opplysninger på ulike vis[1] kan inngå vedkommende myndighets virkeområde. Personvernkommisjonen vil derfor ikke gå nærmere inn på organiseringen av de overnevnte forvaltningsorganer, eller drøfte andre organer som ikke har kontroll med behandling av personopplyninger som sitt primære virkeområde.

I dette kapittelet vil Personvernkommisjonen drøfte organiseringen av de to forvaltningsorganene som har et særlig ansvar i forhold til personopplysningsvernet i Norge, nemlig Datatilsynet og Personvernnemnda.

18.1.1 Rettslig forankring

Datatilsynet ble opprettet den 1. januar 1980, med hjemmel i personregisterloven fra 1978 (opphevet). Fra ikraftredelsen av personopplysningsloven (1. januar 2001) har hjemmelen for Datatilsynets organisering og oppgaver vært å finne i personopplysningsloven § 42. Fra samme tidspunkt ble det administrative ansvaret for Datatilsynet overført fra Justis- og politidepartementet til Arbeids- og administrasjonsdepartementet (jf. kgl. res. 15. des. 2000 nr. 3). Dette departementet heter nå Fornyings- og administrasjonsdepartementet.

Personvernnemnda ble opprettet i 2001 med hjemmel i personopplysningsloven § 43.

Datatilsynet og Personvernnemnda er uavhengige forvaltningsorganer, men er administrativt underlagt Kongen og Fornyings- og administrasjonsdepartementet. Kongen og departementet har ingen instruksjons- eller omgjøringsmyndighet i forhold til enkeltsaker som avgjøres av Datatilsynet og/eller Personvernnemnda. Som ansvarlig departementet for personopplysningsloven vil imidlertid Justisdepartementet kunne avgi generelle tolkningsuttalelser. Tilsvarende gjelder for Fornyings- og administrasjonsdepartementet, som har fått delegert forskriftskompetansen etter personopplysningsloven.

Som en følge av tilpassing av norsk lovgiving i forhold til EUs personverndirektiv (Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995) og overgangen fra personregisterloven til personopplysningsloven i 2001, ble hovedtyngden av Datatilsynets arbeid flyttet fra forhåndskontroll i samband med opprettelse av personregister (konsesjonsbehandling) til en rekke ulike aktiviteter (jf. avsnitt 7.1.2). Tilsynsmyndigheten er nærmere beskrevet i direktivets artikkel 28.

Blant annet fører Datatilsynet tilsyn med, og har vedtakskompetanse i, forhold til behandling av personopplysninger som skjer i medhold av personopplysningsloven, helseregisterloven og den norske delen av SIS-loven, samt forskrifter til disse. Datatilsynets myndighetsområde begrenses blant annet av § 7 i personopplysningsloven, slik at behandling av personopplysninger som skjer for kunstneriske, litterære eller journalistiske, herunder opinionsdannende formål, i hovedsak faller utenfor lovens anvendelsesområde. Det-

[1] Blant oppgavene til Helsetilsynet er for eksempel å etterse at opplysninger i pasientjournaler ikke blir kjent av uvedkommende.

te drøftes mer inngående i kapittel 13, om media og personvern.

Etter personregisterloven kunne Datatilsynets vedtak klages inn for Justisdepartementet. EUs personverndirektiv artikkel 28 nr. 1 krever at imidlertid tilsynsmyndighetene skal være uavhengige. I samband med implementeringen av EU-direktivet opprettet man derfor et uavhengig klageorgan, Personvernnemnda, for vedtak fattet av Datatilsynet i forhold til disse lovene. I tillegg til nevnte lover reguleres Personvernnemndas arbeid av en instruks som departementet har utarbeidet (fastsatt av FAD 31. januar 2002 og revidert 12. januar 2004).

Både Datatilsynet og Personvernnemnda skal årlig orientere Kongen om sitt virke gjennom en årsmelding.

18.1.2 Ledelse, arbeidsoppgaver, budsjett og årsverk

18.1.2.1 Datatilsynet

Datatilsynet ledes av en direktør utnevnt av Kongen. Helge Seip var direktør i tilsynet fra 1980 til 1989. Georg Apenes har ledet Datatilsynet fra 1989 og fram til i dag.

Datatilsynet har mange oppgaver. Disse er nærmere angitt i personopplysningsloven § 42 (3). Bestemmelsen lyder slik:

«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.»

Datatilsynets oppgaver kan etter dette i hovedsak deles inn i fire hovedområder:
- Tilsyns og kontrollvirksomhet.
- Informasjons- og rådgivningsvirksomhet.
- Delta aktivt i den offentlige debatt om spørsmål knyttet til personvern, blant annet gjennom høringsuttalelser til nye lovforslag og utarbeiding av årsmelding.
- Faglig virksomhet.

Som ledd i den faglige virksomheten deltar Datatilsynet i flere internasjonale fora knyttet til personvern og behandling av personopplysninger. Blant annet er tilsynet representert som observatør i EUs fellesorgan for Datatilsyn (Artikkel 29-gruppen, etter artikkel 29 i EUs personverndirektiv), som observatør i den internasjonale arbeidsgruppen for personvern innen telekommunikasjon (Berlin-gruppen), og som observatør ved det felles tilsynsorganet for Schengen Informasjonssystem (Joint Supervisory Authority).

Datatilsynet har altså svært mange og svært vidtspennende oppgaver, fra stedlig tilsyns og kontrollvirksomhet, via rådgivingsvirksomhet, generell informasjonsvirksomhet i samfunnet og deltagelse i samfunnsdebatten, til faglig virksomhet og deltagelse i internasjonale fora, for å ivareta egen og samfunnets kompetanse på området personvern og personopplysningsvern.

I 2007 hadde Datatilsynet 33 årsverk fordelt på fire avdelinger i tillegg til direktøren. Nedenfor gis en oversikt over bemanning, samt faglig bakgrunn for de som er tilknyttet de ulike avdelingene (data hentet far Datatilsynets hjemmeside 2008-10-06).
- Direktøren (jurist)
- Informasjonsavdelingen: 8 medarbeidere (4 jurister, 4 informasjonsarbeidere)
- Juridisk avdeling: 13 medarbeidere (13 jurister)
- Tilsyns- og sikkerhetsavdelingen: 5 medarbeidere (4 ingeniører, 1 samfunnsviter)
- Administrasjonsavdelingen: 7 medarbeidere (bakgrunn ikke oppgitt)

På Datatilsynets hjemmesider (Datatilsynet 2008a) beskrives avdelingenes arbeidsoppgaver som følger:

Tabell 18.1

År	Budsjett (MNOK)	Faste stillinger	Kostnad pr. årsverk (TNOK)
2001	18,4	26	710
2002	17,8	27	660
2003	18,3	26	700
2004	21	27	780
2005	23	31	740
2006	24,8	32	780
2007	25	33	760

«*Informasjonsavdelingens* medarbeidere har som hovedoppgave å få ut informasjon om Datatilsynets arbeid til folk flest. De aller fleste henvendelser fra publikum til Datatilsynet via telefon, brev eller e-post blir kanalisert til Datatilsynets juridiske svartjeneste. De fire juristene svarer på alle mulige tema innen personvern. De øvrige ansatte på avdelingen har ansvar for mediekontakt og nettsidene, bistår i ulike prosjekt og i arbeidet med å lage veiledere om ulike tema. Avdelingen tar også imot forespørsler om foredrag og gjør annet løpende informasjonsarbeid.

Datatilsynets [*juridiske avdeling*] driver hovedsakelig med saksbehandling. Det kan dreie seg om enkeltvedtak, høringer og rapportskriving. Mye tid går med til tilsynsvirksomhet. I tillegg stiller juristene jevnlig som deltakere og foredragsholdere på kurs og konferanser. Internasjonalt samarbeid prioriteres også høyt.

Tilsyns- og sikkerhetsavdelingen, har i tillegg til IT driftsoppgaver og teknisk saksbehandling, ansvar for organiseringen av tilsynsvirksomheten. Det innebærer tilsyn hos forskjellige virksomheter, med kontroll av behandlinger av personopplysninger. Avdelingen gir råd og veiledning, både skriftlig og muntlig, om informasjonssikkerhet og tekniske spørsmål rundt personvern. Den er også aktiv i utvikling av bransjenormer, og arrangerer rådgivningsuker der representanter fra ulike virksomheter får hjelp og bistand i spørsmål som har med sikkerhet å gjøre.

De syv ansatte [i *administrasjonsavdelingen*] har ansvar for lønn, regnskap, budsjett, sentralbord, arkiv, bibliotek, internkontroll og rapporteringer i forhold til departementet, i tillegg til ansvar for alle fellesfunksjoner. Avdelingen har personalansvar, behandler innsynsbegjæringer og deltar i og koordinerer planarbeid.»

Tabellen over gjengir Datatilsynets budsjett og antall faste stillinger (tallene er hentet fra tilsynets årsmeldinger de siste syv årene).

18.1.2.2 Personvernnemnda

Personvernnemnda har syv medlemmer som oppnevnes på åremål for fire år av gangen, med adgang til gjenoppnevning for ytterligere fire år. Lederen og nestlederen oppnevnes av Stortinget. De øvrige fem medlemmene oppnevnes av Kongen. Siden oppstarten i 2001 har Personvernnemnda vært ledet av professor, dr. juris Jon Bing.

Nemnda skal avgjøre klager over Datatilsynets avgjørelser. Nemnda kan videre omgjøre avgjørelser etter eget tiltak i henhold til forvaltningsloven § 35.

For å sikre en reell to-instansbehandling av saker, skal nemnda ikke være involvert i Datatilsynets saksbehandling, og omvendt. Nemnda kan be Datatilsynet om å skaffe til veie faktiske opplysninger i saker nemnda har til behandling.

Personvernnemnda møtes normalt en gang i måneden, og fatter fortløpende vedtak knyttet til mottatte klager. Personvernnemnda kan bestemme at lederen eller nestlederen sammen med to andre nemndmedlemmer kan behandle klager over avgjørelser som må avgjøres uten opphold. Søksmål om gyldigheten av Personvernnemndas avgjørelser rettes mot staten ved Personvernnemnda.

18.2 Personvernkommisjonens observasjoner

18.2.1 Om begrepene «ombud» og «tilsyn»

Ordet «ombud» kommer av norrønt umboð, som betyr «fullmakt». Den moderne bruken av ordet stammer fra Sverige – nærmere bestemt fra 1809 da den første svenske ombudsmann ble oppnevnt av Riksdagen for å ivareta enkeltpersoners rettig-

heter vis a vis offentlig myndighetsutøvelse (Ombudsman 2008).

I Norge har vi følgende statlige ombud: Barneombudet, Ombudsmannen for forsvaret, Likestillings- og diskrimineringsombudet, Forbrukerombudet, Sivilombudsmannen. Videre finnes det pasientombud på fylkesnivå og, som en frivillig ordning, eldreombud på kommunalt nivå. Det finnes også en rekke ombudsfunksjoner som ikke har offentligrettslig karakter, som personvernombud, leserombud og verneombud. Slike ombud faller utenfor denne drøftelsen.

I norsk forvaltning benyttes ombudsordninger gjerne for å styrke og ivareta interessene til svake grupper i samfunnet, eller som talspersoner på områder der det er generelt behov for vern av enkeltpersoner.

Ombud ivaretar ulike oppgaver, som å delta i den offentlige debatt, bidra med informasjon og synspunkter i forbindelse med høringer, veilede og rettlede, men har også oppgaver knyttet til vurdering av saksbehandlingen i enkeltsaker, ivaretakelse av enkeltpersoners interesser i konkrete saker, samt generell overvåkning og kontroll med forvaltningens og andres virksomhet.

De uttalelser som et tradisjonelt ombud måtte komme med vil som regel være av en anbefalende eller saksopplysende karakter. Uttalelsene er ikke bindende for dem de er rettet mot. For mange av ombudene er det imidlertid tilknyttet organer (for eksempel Markedsrådet som behandler uttalelser fra Forbrukerombudet) som kan treffe avgjørelser som er bindende med mindre de bringes inn til behandling for domstolene.

For en grundigere drøfting av ombudsbegrepet i norsk forvaltning, se for eksempel Fauchald (2004, s. 829).

Det er påfallende lite å finne i forvaltningsrettslig litteratur om tilsyn, men Erik Boe (1993, ss. 466, 859-863) har følgende å si om pliktene og ansvaret som følger av det å ha tilsyn:

1. Tilsynsplikten:
   a) Plikten til å sørge for å bli skikkelig orientert om det som foregår.
   b) Plikten til å påse at ressursbruk, handlinger og myndighetsutøvelse holder mål.
   c) Plikten til å følge med i det som underordnede gjør.
2. Tilsynsansvar:
   a) Plikten til å avklare forhold som kan være kritikkverdige.
   b) Plikten til å rydde opp i uregelmessigheter.
   c) Plikten til å reagere skikkelig når snusk og misligheter oppdages.

Boe påpeker videre at det ikke finnes noen generell lovbestemmelse om forvaltningens ansvar, med unntak av kommuneloven som har regler om tilsyn. Tilsynsplikt er ikke desto mindre en selvfølgelig del av virket til ethvert forvaltningsorgan. Vi kan snakke om et alminnelig tilsynsansvar. Ansvaret følger av posisjonen som overordnet myndighet.

Personvernkommisjonen mener ut fra dette at det kan sondres mellom et ombud og et tilsyn. Mens en ombudsfunksjon er knyttet til ivaretakelse og styrking av bestemte interesser, innebærer det å ha tilsyn med et område en plikt til å følge med i hva som foregår og et ansvar for å gripe inn og korrigere feil og uregelmessigheter, dersom kompetansen til å gripe inn ligger innenfor tilsynets mandat.

Datatilsynets plassering i forhold til dette ble drøftet i forarbeidene til personopplysningsloven (Ot.prp. nr. 92 (1998-99) punkt 13.3.5), hvor det heter at:

> «Etter § 42 i lovforslaget kan Datatilsynets oppgaver i hovedsak deles inn i to hovedområder; kontroll- og tilsynsvirksomhet på den ene siden og informasjons- og rådgivningsvirksomhet på den andre. I tillegg kommer oppgaver som å delta aktivt i den offentlige debatt om spørsmål knyttet til personvern, blant annet gjennom høringsuttalelser til nye lovforslag og utarbeiding av årsmelding om sin egen virksomhet. Når man ser hen til disse oppgavene, er det ikke naturlig å karakterisere tilsynet som en ombudsinstans slik ombudsfunksjonen tradisjonelt er utformet. Som det fremgår bl.a. av §§ 42, 46 og 47 i lovforslaget tillegges Datatilsynet en kontroll- og tilsynsfunksjon med adgang til å utferdige pålegg og ilegge tvangsmulkt. Datatilsynet skal også behandle konsesjonssøknader, jf. § 33 i forslaget. Dette er en type forvaltningsmyndighet som går utover det som tradisjonelt er vanlig for et ombud. Departementet mener at det på denne bakgrunn er mest naturlig å karakterisere Datatilsynet som et forvaltningsorgan som skal være faglig uavhengig av regjeringen eller som et forvaltningsorgan med særskilt vide fullmakter.» [Vår utheving.]

På sin egen hjemmeside (Datatilsynet 2008b) betegner tilsynet seg både som et ombud og som et tilsyn.:

> «Datatilsynet er oppretta for å sjå til at personopplysningslova vert fulgt. Formålet med lova er å verne den einskilde mot krenking av personvernet gjennom bruk av personopplysningar. Datatilsynet er både tilsyn og ombud.»

I sin årsmelding (2008e, s. 7), skriver Datatilsynet dette:

> «Sist, men ikke minst, har Datatilsynet også en viktig ombudsrolle. I den forbindelse drives rådgivning og informasjon overfor enkeltpersoner som tar kontakt med tilsynet. Publikum generelt nås i første rekke gjennom aktiv mediekontakt og publisering på eget nettsted. For å skape oppmerksomhet og interesse omkring personvernspørsmål deltar Datatilsynet aktivt i den offentlige debatt og legger stor vekt på å praktisere meroffentlighet.»

Av EUs personverndirektiv artikkel 28, fremgår det at tilsynsmyndigheten skal overvåke anvendelsen av loven, og herunder gripe inn og bringe ulovlige behandlinger til opphør. For øvrig gir direktivet personvernmyndighetene stort handlingsrom.

Når det gjelder personvernmyndighetene i andre land i EØS-området, har Personvernkommisjonen merket seg at det er vanlig praksis at disse er tilsyn som også fyller en ombudsfunksjon.

Det er ingen tvil om at Datatilsynet oppfatter at deres oppgave er å ivareta personvernet og være en talsperson overfor andre offentlige myndigheter og private aktører både når det gjelder personopplysningsvernet og generelt vern av den personlige integritet. Personvernkommisjonen mener at dette er en viktig oppgave og at personvernet i møte med andre interesser absolutt trenger noen som taler personvernets sak og som tør å kritisere både offentlige myndigheter og private aktører når de på ulike måter utfordrer personvernet.

Det er imidlertid ikke uproblematisk at det forvaltningsorganet som treffer enkeltvedtak og utøver myndighet etter personopplysningsloven, er det samme organet som er gitt i oppgave å tale personvernets sak. Den konkrete myndighetsutøvelsen etter personopplysningsloven forutsetter en avveining av mange ulike interesser, og det kan i noen tilfeller være uheldig at avveiningen foretas av et organ som oppfatter at deres oppgave er å ivareta én spesiell interesse fremfor en annen. Personvernkommisjonen utelukker ikke at dette kan være en mulig forklaring på den store omgjøringsprosenten ved klagesaker i Personvernnemnda enkelte år, og viser i den forbindelse særlig til at Personvernnemnda er et kollegialt organ satt sammen av personer med ulik bakgrunn nettopp for å sikre en bred interesse- og fagrepresentasjon. Personvernkommisjonen kommer tilbake til dette nedenfor.

18.2.2 Om vedtak i Datatilsynet og Personvernnemnda

Datatilsynets vedtak kan som nevnt påklages til Personvernnemnda. Resultatet i slike klagesaker fremgår blant annet av Datatilsynet og Personvernnemndas årsmeldinger, i tillegg til at de offentliggjøres på Personvernnemndas nettsted.

Som det fremgår av tabellen under, er det forholdsvis få saker som blir påklaget, men av de sakene som klages inn for nemnda er omgjøringsprosenten relativt høy i enkelte år:

Så langt i 2008 er bare to klagesaker behandlet. I begge sakene ble Datatilsynets vedtak omgjort av Personvernnemnda.

Personvernkommisjonen ønsker ikke å spekulere i årsakene til den faglige uenigheten som i enkelte år har gjort seg gjeldene, men mener at en så stor omgjøringsprosent er bekymringsverdig, da den innebærer en viss grad av uforutsigbarhet i saksbehandlingen og derfor kan utgjøre et rettssikkerhetsproblem. Dette er bakgrunnen for at Personvernkommisjonen foreslår at det opprettes et kollegialt rådgivende organ i Datatilsynet med funksjon i forbindelse med klagesaker, se nedenfor.

Tabell 18.2

År	Klager ferdigbehandlet i Nemnda	Vedtak helt eller delvis ble omgjort	Omgjøring i %
2007	7	1	14 %
2006	15	7	41 %
2005	9	5	56 %
2004	6	3	50 %
2003	6	2	33 %
2002	6	1	17 %
2001	1	0	0 %

18.2.3 Om Personvernnemnda

Personvernkommisjonen ser ingen grunn til å endre på Personvernnemndas organisering eller mandat. Vi legger derfor til grunn at denne videreføres i sin nåværende form, og at leder og medlemmer fortsatt oppnevnes på åremål (4 år med mulighet for én gjenoppnevning).

18.2.4 Om direktørens tilsettingsform

Personvernkommisjonen har merket seg at et samlet lovutvalg gikk inn for at Datatilsynets direktør bør være en embetsmann som utnevnes av regjeringen, og at regjeringen har anledning til å ansette direktøren på åremål (jf. Ot.prp. nr. 92, 1998-99, punkt 13):

> «[d]epartementet slutter seg til utvalgets forslag om at Datatilsynets direktør også i fremtiden bør være en embetsmann. Departementet er videre enig med utvalget i at gode grunner kan tale for å gi regjeringen anledning til å utnevne direktøren på åremål. Direktøren får et stort selvstendig ansvar for Datatilsynets virksomhet. Stillingen stiller krav til variert erfaringsbakgrunn, omstillingsevne og faglig fornyelse. Da Stortinget i 1992 endret Grunnloven § 22 tredje ledd dit hen at det kan bestemmes ved lov at også embetsmenn kan utnevnes på åremål, ble nettopp disse momentene fremhevet som beveggrunner for endringen. De fleste topplederne som er ansatt som tjenestemenn i forvaltningsbedriftene og direktoratene er ansatt på åremål. Det samme gjelder f.eks. direktøren for Kredittilsynet og Konkurransetilsynet samt de ulike ombudene. På samme måte som for andre lederstillinger vil det styrke ledelsen av Datatilsynet at topplederen ikke sitter for lenge. En viss rotasjon i topplederstillingen vil på sikt kunne sikre en administrativ og faglig nyskaping. Dette er særlig viktig når man styrker Datatilsynets uavhengighet og fjerner den politiske kontrollen i faglige spørsmål. Adgangen til å utnevne på åremål kan ikke gjøres gjeldende for den nåværende direktøren i Datatilsynet.»

Personvernkommisjonen mener at man på samme måte som for andre lederstillinger vil kunne styrke ledelsen av Datatilsynet dersom topplederen har en tidsbegrenset funksjon. En viss rotasjon i topplederstillingen vil på sikt kunne sikre en administrativ og faglig nyskaping. Dette er særlig viktig ettersom Datatilsynets er et uavhengig tilsynsorgan og ikke underlagt politisk kontroll i faglige spørsmål.

Direktøren for Datatilsynet bør derfor ansettes på åremål, slik at lovgivers intensjoner med hensyn til stillingen oppnås, (jf. Ot.prp. nr. 92, 1998-99, punkt 13) – enten for 4 år med adgang til én gjenoppnevning, eller for 8 år.

18.2.5 Om tilsynets profesjonssammensetning

Når det gjelder bemanningen av Datatilsynet, så består den delen av staben som har profesjonsbakgrunn i dag av 18 jurister, 4 ingeniører og 1 samfunnsviter.

Personvernkommisjonen har ikke hatt anledning til å sette seg inn i det daglige arbeidet i Datatilsynet, og ønsker av den grunn ikke å gå detaljert inn på tilsynets sammensetning rent faglig sett. På generelt grunnlag har imidlertid Personvernkommisjonen observert at personvernet ser ut til å møte en rekke nye utfordringer som følge av rask teknologisk utvikling og som følge av nye media. Samtidig utvikles det stadig ny teknologi som gjør det mulig å gi personverninteressene et bedre vern, noe som også krever kontinuerlig oppdatering på fagområdet. Dette kan tilsi at Datatilsynet bør få tilført flere ressurser med teknologisk kompetanse.

18.2.6 Om personvernombudene

I Sverige finnes det om lag 3284 personvernombud. I Norge ble ordningen med personvernombud introdusert med ikrafttredelse av personopplysningsloven, og antall personvernombud her i landet er i skrivende stund 118, som dekker til sammen 304 virksomheter. Et personvernombud er en ressursperson som enten er ansatt i virksomheten som behandler personopplysninger, eller er en ekstern person, som blant annet har til oppgave å:

- Føre oversikt over virksomhetens behandling av personopplysninger.
- Påse at ledelsen i virksomheten har etablert et system for internkontroll.
- Bistå personer som er registrert (datasubjekter).
- Besvare spørsmål om personvern internt i virksomheten.
- Påpeke brudd på personopplysningsloven overfor ledelsen.
- Være kontaktperson ved henvendelser fra Datatilsynet.
- Holde seg orientert om utviklingen innen personvern.

Virksomheter med personvernombud får dessuten fritak fra Datatilsynet fra lovpålagt meldeplikt om behandling av personopplysninger. I stedet mottar personvernombudet meldingen om, og kvalitetssikrer behandlingen vis à vis behandlingsansvarlig.

Datatilsynet driver kontinuerlig kompetanseoppbyggende virksomhet ovenfor personvernombudene, blant annet gjennom et obligatorisk seminar for nyoppstartede personvernombud, og gjennom løpende informasjonsvirksomhet.

Personvernkommisjonen mener ikke at det bør være noe mål å etablere et svært stort antall personvernombud, slik man har gjort i Sverige. For mange ombud kan medføre at Datatilsynet ikke har kapasitet til å gi personvernombudene tilstrekkelig oppfølgning og rådgivning, noe som i verste fall kan innebære en svekkelse av personvernet.

Personvernkommisjonen mener at ordningen med personvernombud slik den fungerer i Norge i dag er forholdsvis tilfredsstillende, og at Datatilsynet bør fortsette å vektlegge kvalitet fremfor kvantitet i oppfølgingen av personvernombudene.

18.3 Forslag til tiltak

Nedenfor følger kommisjonens konkrete forslag til tiltak som bør iverksettes med tanke på fremtidig organisering av personvernmyndighetene.

18.3.1 Oppgaver

Et flertall i kommisjonen (14 medlemmer) mener at Datatilsynet bør videreføre sine fire hovedarbeidsområder med arbeidsoppgaver som kombinerer tilsyns- og ombudsvirksomhet.

Et mindretall (1 medlem, Rune Fløisbonn) mener at det er problematisk at dagens Datatilsyn som utøver myndighet etter personopplysningsloven, også er gitt i oppgave å tale personvernets sak, og ofte gjør det innenfor snevre hensynsrammer.

Mindretallet mener arbeidet med personvernspørsmål styrkes ved at blir et organisatorisk skille mellom tilsynsoppgaver og ombudsoppgaver. Mindretallet mener at Datatilsynet bør omgjøres til et Personverntilsyn som underlegges Justisdepartementet som et forvaltningsorgan med klare linjer i forhold til tilsynets rolle, oppgaver og administrativ styring. Personverntilsynet bør få en styrket faglige bemanning, men konsentrere sin virksomhet innenfor tilsynsoppgaver, treffe enkeltvedtak og utøve myndighet etter personopplysningsloven.

Mindretallet foreslår samtidig at Stortinget oppnevner et frittstående personombud som taler personvernets sak, behandler klager, samt gir råd og bistand. Mindretallet foreslår endring av navn på forvaltningsorganet fra Datatilsynet til «Personverntilsynet» for både å markere oppgaveendringer i forhold til dagens Datatilsyn og hindre navn- og oppgavesammenblanding med «Post og teletilsynet», som også er et datatilsyn.

18.3.2 Økte ressurser til Datatilsynet

Personvernkommisjonen mener at Datatilsynet har for begrensede ressurser i forhold til de omfattende oppgavene de er tillagt og som de påtar seg. Dette bør løses ved at Datatilsynet blir tilført tilstrekkelige ressurser. Det er ikke ønskelig å løse ressurssituasjonen ved å redusere omfanget av tilsynets oppgaver.

Teknologiutviklingen og utbredelsen av nye media basert på informasjons- og informasjonsteknologi vil i tiden som kommer utfordre personvernet, men også skape muligheter for et bedre personvern og et sterkere personopplysningsvern. For å møte disse utfordringene og ivareta teknologiske muligheter, mener Personvernkommisjonen at man må ha et særlig fokus på hvordan Datatilsynets kompetanse og kapasitet i forhold til denne utviklingen kan sikres og styrkes.

Personvernkommisjonen ønsker at Datatilsynet generelt sett får tilført flere ressurser, og at noe av denne økningen skjer ved en bredere representasjon av ulike interesser i Datatilsynets profesjonelle stab, inklusive mediefaglige, samfunnsfaglige og IKT-faglige interesser. Uten at nedstående oversikt er å betrakte som uttømmende, vil Personvernkommisjonen foreslå at man særlig ser på hvordan følgende spesifikke områdene kan styrkes i samband med nyrekruttering:

- identitetsforvaltning, personvernfremmende teknologier (se rapportens kapittel 10);
- nye media, inklusive web 2.0-teknologi (se rapportens kapittel 13);
- design av informasjonssystemer og informasjonssikkerhet.

18.3.3 Regionalisering av Datatilsynet

Personvernkommisjonen ser det som en hensiktsmessig mulighet at en vesentlig del av ressursøkningen i Datatilsynet skjer gjennom regionalisering. Eksempelvis kan det opprettes fem regionale

«Datatilsyn», ett i hver landsdel, som har et særlig ansvar for gjennomføring av tilsyn innenfor sin region, behandling av meldinger om installering av overvåkningskameraer, oppfølging av lokale personvernombud, lokal rådgivings- og informasjonsvirksomhet etc. Personvernkommisjonen mener at en slik lokal tilknytning vil tilføre viktige perspektiver når man skal vurdere for eksempel hensiktsmessigheten og behovet for et overvåkningstiltak, velge ut relevante tilsynsobjekter og utvikle en relevant informasjonsstrategi for dette området.

Det bør også vurderes om regionale tilsyn som er lokalisert i nærheten av et akademisk miljø med særlig kompetanse på et bestemt område (for eksempel miljøet ved NTNU og Uninett i Trondheim som arbeider med datasikkerhet og identitetsforvaltning), skal gis ansvaret for å forvalte Datatilsynets kompetanse på relevante områder.

For å sikre et tilstrekkelig bredt fagmiljø er det viktig at de regionale Datatilsyn ikke blir for små. Hvert regionkontor bør derfor ha en bemanning på minst seks personer.

18.3.4 Et råd for Datatilsynet

Personvernkommisjonen mener at det bør opprettes et «Datatilsynets råd» som kan fungere som et kollegialt rådgivingsorgan med en bredere sammensatt kompetanse enn den man finner i Datatilsynets profesjonelle stab. Behovet for et slikt råd må sees i samband med det vi tidligere (avsnitt 7.1) har skrevet om at personopplysningsloven fordrer mange interesseavveininger, og at man bør sikre at også andre interesser enn personverninteresser blir tilfredsstillende vektlagt. Formålet med et slikt råd skal være kvalitetssikring knyttet til særlig vanskelige og prinsipielle saker og klagesaker.

18.3.5 Sektorvis styrking av personvernkompetansen

Personvernkommisjonen vil foreslå en sektorvis styrking av personvernkompetansen ved at andre forvaltningsorganer som kommer i berøring med personvernproblemer (som for eksempel Arbeidstilsynet, Helsetilsynet og Utdanningsdirektoratet) har en person internt med høy personvernfaglig kompetanse og da særlig i forhold til personvernspørsmål som er relevante for dette organet. Rent konkret kan dette skje ved at det oppnevnes personvernombud i de berørte etatene (der slike ikke allerede finnes), og at disse ombudene gis relevant opplæring og oppfølgning.

18.3.6 Samarbeide med eksterne aktører

Personvernkommisjonen har registrert at Datatilsynet med hell har gjort bruk av flere kontaktflater mot eksterne aktører for å nå fram til publikum med informasjons- og holdningsskapende arbeide. Vi tror at suksessen til kampanjer som *Dubestemmer* til dels skriver seg fra dette, og ikke minst at man gjennom kampanjen har vært dyktig i å involvere de den angår (her: barn og unge).

Personvernkommisjonen tror at slike samarbeidsprosjekter også vil være viktige i fremtiden, og at Datatilsynet på denne måten kan få til en tettere dialog som blant annet gir budskapet større troverdighet og gjennomslagskraft i forhold til de aktuelle målgrupper.

18.3.7 Dialog med akademia og andre fagmiljøer

I forlengelsen av dette mener Personvernkommisjonen at Datatilsynet også bør sørge for at tilsynet har løpende kontakt med akademia (universiteter, høyskoler og forskningsinstitusjoner).

Siktemålet med dette tiltaket er tosidig. Dels skal dette bidra til å øke oppmerksomheten hos ansatte i disse institusjonene omkring personvernspørsmål, dels utgjøre et grunnlag for gjensidig kompetanseoverføring mellom Datatilsynet og akademia.

Personvernkommisjonen ønsker ikke å legge bestemte føringer på hvordan dette skal skje, men som eksempler på slike kontaktflater kan vi nevne:

- Datatilsynet kan tilskynde, og gjerne delta i, forskningsprosjekter omkring personvernrelevante emner.
- Datatilsynet kan delta i de åpne faglige interessefellesskap (gjerne organisert rundt e-postlister) som finnes i akademia og som har fokus på personvern, herunder også ny teknologi og nye media som er særlig relevant i forhold til personvern.
- I slike faglige interessefellesskap arrangeres det også seminarer og workshops. Ved å delta aktivt på slike kan Datatilsynet tilskynde til dialog og til utveksling av kompetanse.

En slik kontakt må selvsagt være gjensidig. For at kontakten skal være produktiv, må både Datatilsynet og akademia ta et ansvar for å etablere og vedlikeholde forbindelsen.

Kapittel 19
Grunnlovsfesting av personvernet

19.1 Bakgrunn

Grunnlovsfesting av personvernet er et viktig politisk tema og har lenge vært en del av den offentlige debatten. Spørsmålet ble blant annet diskutert i forbindelse med at Ytringsfrihetskommisjonen avga sin innstilling med forslag til endring av bestemmelsen om ytringsfrihet i Grunnloven § 100. Høsten 2008 fremsatte Venstre et forslag om å grunnlovsfeste privatlivets fred og vern av personopplysninger.

På Personvernkommisjonens åpne seminar om media og personvern var det flere av deltakerne som påpekte behovet for grunnlovsfesting av personvernet. Fokuset var særlig den ubalansen det gir at ytringsfrihet er grunnlovsfestet, men ikke personvernet, når disse interessene regelmessig står i et motsetningsforhold. Det er også et faktum at den digitale utviklingen har gitt, og vil fortsette å gi, nye utfordringer for personvernet. Dette gir spørsmålet om grunnlovsfesting særlig aktualitet i dagens samfunn.

På bakgrunn av dette ga Personvernkommisjonen Alf Petter Høgberg og Njål Høstmælingen i oppdrag å skrive en betenkning som drøfter fordeler og ulemper ved grunnlovsfesting av retten til personvern/privatliv. Hele utredningen er tatt inn som vedlegg 3. Her vil Personvernkommisjonen fremheve de momentene som underbygger vår konklusjon om at personvernet bør grunnlovsfestes i Norge.

19.2 Kort om utredningen

Utredningen starter med en begrepsavklaring, som etter Personvernkommisjonens oppfatning har til formål å avklare hva som skal grunnlovsfestes: personvern i vid forstand, herunder retten til privatliv og personopplysningsvern, eller om grunnlovsvernet bør forbeholdes en snevrere definisjon av privatlivets fred.

Forfatterne konkluderer med at det ikke er nødvendig å trekke noe klart skille mellom personvern og privatliv og legger til grunn at personopplysningsvernet uansett omfattes av disse begrepene. De knytter sin vurdering opp mot hva som innholdsmessig kan utledes av EMK artikkel 8 slik denne er tolket blant annet gjennom praksis fra EMD.

For å gi en nærmere oversikt over omfanget av hva slags interesser en eventuell grunnlovsbestemmelse skal beskytte, gis det en fremstilling av noen konkrete forhold som reguleres av privatlivsbestemmelsen i EMK. Det gis også en oversikt over hvilke regler som styrker borgernes personvern etter norsk rett, både i dagens Grunnlov, formell lov, ulovfestede prinsipper, praksis og reelle hensyn.

I utredningens kapittel 4 gjøres det en såkalt konsekvensanalyse, det vil si en gjennomgang av noen sentrale hensyn som taler for og imot en grunnlovsfesting av personvernet.

Forfatterne konkluderer med at retten til personvern/privatliv bør grunnlovsfestes. Det legges særlig vekt på at en grunnlovsfesting vil synliggjøre personvernet som rettslig skranke og ha sentral verdi ved lovgivning og rettsanvendelse. I tillegg fremheves det at man vil oppnå bedre balanse i Grunnlovens eksisterende rettighetsvern. De hensyn som taler i mot grunnlovsfesting, mener forfatterne i stor grad vil kunne avhjelpes i forbindelse med utforming av bestemmelsen. Blant annet påpekes det at man bør tilstrebe en rimelig balanse mellom presisjonsnivå og abstraksjonsnivå og at grunnlovsbestemmelsen bør forankres i de menneskerettslige kjernebestemmelser, slik at man får med seg utviklingen og dynamikken i folkeretten.

19.3 Personvernkommisjonens vurdering

Grunnloven har stor rettslig og politisk betydning, i tillegg til at den har en vesentlig symbolef-

fekt både for borgerne og staten. Grunnlovsfesting av personvernet vil medføre at personvernet får en sentral rolle i konkrete saksforhold samtidig som man presiserer at også individuelle rettigheter er en viktig del av vår rettstat.

Flere steder i denne rapporten har Personvernkommisjonen gitt en oversikt over lovverk som enten har til formål å ivareta personvernet direkte eller som får en indirekte betydning for enkeltpersoners privatliv eller håndteringen av deres personopplysninger. Lovgivningen er til dels fragmentarisk og spredt. Ettersom personopplysninger behandles innenfor de fleste sektorer og bransjer, finnes det i tillegg en rekke lover og forskrifter som får konsekvenser for personvernet uten at det nødvendigvis er dokumentert at lovgiver har sett hen til sentrale personverninteresser ved vedtagelsen.

Personvernkommisjonen mener at en grunnlovsfesting av personvernet vil kunne styrke vektleggingen av personverninteresser når man vedtar nye lover og i lovgivningsprosessen, da lovgiver vil tilstrebe at lovgivningen ikke er grunnlovsstridig.

Personvernkommisjonen vil også fremheve den betydningen Grunnloven har som rettskilde etter norsk rett. Det er nærliggende å tro at man ved tolkningen av andre lover vil tillegge personverninteresser større vekt dersom disse kan utledes av Grunnloven. På denne måten sikrer grunnlovsfesting av personvernet at personvernhensyn blir en sentral del av vår rettsanvendelse.

Spesielt i kapittel 13 om media og personvern har Personvernkommisjonen pekt på at ytringsfriheten og personvernet er to sentrale menneskerettigheter som kan stå i et motsetningsforhold. Ettersom ytringsfriheten er gitt beskyttelse i Grunnloven, er det en reell fare for at denne rettigheten vil bli gitt forrang eller anses for å ha det sterkeste vernet når personvernet og ytringsfrihetene skal veies opp mot hverandre i konkrete saker. For å skape balanse mellom to likeverdige interesser mener Personvernkommisjonen det vil være av sentral og praktisk betydning å grunnlovsfeste også personvernet.

Når det gjelder eventuelle ulemper ved en grunnlovsfesting, vises det til utredningens kapittel 4. Personvernkommisjonen vil særlig fremheve betydningen av at man utarbeider en grunnlovstekst som er egnet til å avhjelpe slike ulemper. Det må særlig tilstrebes at teksten gis en form som er egnet til å imøtekomme den rettsutviklingen som skjer internasjonalt gjennom tolkning og presisering av EMK, samtidig som bestemmelsen får den nødvendige klarhet som må til for at den kan få betydning i konkrete saker.

19.4 Konklusjon

Personvernkommisjonen anbefaler at personvernet, herunder retten til privatliv og personopplysningsvernet grunnlovsfestes i Norge.

Personvernkommisjonen mener at dette arbeidet bør prioriteres og gjøres uavhengig av en totalrevisjon av Grunnloven.

Direktiver omtalt i rapporten

Datalagringsdirektivet: Direktiv 2006/24/EF av 15. mars 2006 om lagring av data generert eller behandlet i forbindelse med tilblivelse av offentlig tilgjengelige elektroniske kommunikasjonstjenester eller elektroniske kommunikasjonsnett og om endring av direktiv 2002/58/EF.

Draft Commission Regulation supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008 (DOO1258/02), tilgjengelig ved http://www.statewatch.org/news/2008/sep/eu-com-aviation-security.pdf (sist besøkt 2008-11-12).

EFC-direktivet: Directive 2004/52/EF of 29 April 2004 on the Interoperability of Electronic Road Toll Systems in the Community.

Ehandelsdirektivet: Direktiv 2000/31/EF.

Kommunikasjonsverndirektivet: Direktiv 2002/58/EF av 12. juli 2002 om behandling av privatlivets fred innen området for elektronisk kommunikasjon.

Personverndirektivet, 95/46/EF av 24. oktober 1995.

Lover og forskrifter omtalt i rapporten

Lover

Adoposjonsloven: *Lov om adopsjon* av 28. februar 1986 nr. 8.

Arbeidsmarkedsloven: *Lov om arbeidsmarkedstjenester* av 10. desember 2004 nr. 76.

Arbeids- og velferdsforvaltningsloven: *Lov om arbeids- og velferdsforvaltningen* av 16. juni 2006 nr. 20.

Arbeidsmiljøloven: *Lov om arbeidsmiljø, arbeidstid og stillingsvern* mv av 17. juni 2005 nr. 62.

Arkivloven: *Lov om arkiv* av 12. april 1992 nr. 126.

Barnehageloven: *Lov om barnehager* av 17. juni 2005 nr. 64.

Barneloven: *Lov om barn og foreldre* av 8. april 1981 nr. 7.

Barnevernloven: *Lov om barneverntjenester* av 17. juli 1992 nr. 100.

Biobankloven: *Lov om biobanker* av 21. februar 2003 nr. 12.

Bioteknologiloven: *Lov om humanmedisinsk bruk av bioteknologi m.m.* av 5. desember 2003 nr. 100.

Diskrimineringsloven: *Lov om forbud mot diskriminering på grunn av etnisitet, religion mv.* av 3. juni 2005 nr. 33.

Domstolloven: *Lov om domstolene* av 13. august 1915 nr. 5.

Ehandelsloven: *Lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester* av 23. mai 2003 nr. 35.

Ekomloven: *Lov om elektronisk kommunikasjon* av 4. juli 2003 nr. 83.

Eksportkontrolloven: *Lov om kontroll med eksport av strategiske varer, tjenester og teknologi av* 18. desember 1987 nr. 93.

Folkeregisterloven: *Lov om folkeregistrering* av 16. januar 1970 nr. 1.

Folketrygdloven: *Lov om folketrygd* av 28. februar 1997 nr. 19.

Forbrukerkjøpsloven: *Lov om forbrukerkjøp* av 21. juni 2002 nr. 34.

Forskningsetikkloven: *Lov om behandling av etikk og redelighet i forskning* av 30. juni 2006 nr. 56.

Forvaltningsloven: *Lov om behandlingsmåten i forvaltningssaker* av 10. februar 1967.

Grunnloven: *Kongeriget Norges Grundlov, given i Rigsforsamlingen paa Eidsvold den 17de Mai 1814* av 17. mai 1814.

Helseforskningsloven: *Lov om medisinsk og helsefaglig forskning* av 20. juni 2008 nr. 44

Helsepersonelloven: *Lov om helsepersonell m.v.* av 2. juli 1999 nr. 64.

Helseregisterloven: *Lov om helseregister og behandling av helseopplysninger* av 18. mai 2001 nr. 24.

Kommuneloven: *Lov om kommuner og fylkeskommuner* av 25. september 1992 nr. 107.

Likestillingsloven: *Lov om likestilling mellom kjønnene* av 9. juni 1978 nr. 45.

Ligningsloven: *Lov om ligningsforvaltning* av 13. juni 1980 nr. 24.

Lov om redaksjonell fridom i media av 13 juni 2008 nr. 41.

Luftfartsloven: *Lov om luftfart* av 11. juni 1993 nr. 101.

Markedsføringsloven: *Lov om kontroll med markedsføring og avtalevilkår* av 16. juni 1972 nr. 47.

Menneskerettsloven: *Lov om styrking av menneskerettighetenes stilling i norsk rett* av 21. mai 1999 nr. 30.

NAV-loven: *Lov om arbeids- og velferdsforvaltningen* av 16. juni 2006 nr. 20.

Offentlighetsloven: *Lov om offentlighet i forvaltningen* av 19. juni 1970 nr. 69.

Opplæringsloven: *Lov om grunnskolen og den vidaregåande opplæringa* av 17. juli 1998 nr. 61.

Pasientrettighetsloven: *Lov om pasientrettigheter* av 2. juli 1999 nr. 63.

Personopplysningsloven: *Lov om behandling av personopplysninger* av 14. april 2000 nr. 31.

Personregisterloven: *Lov om personregistre m.m.* av 9. juni 1978 nr. 48 (opphevet).

Pliktavleveringsloven: *Lov om avleveringsplikt for allment tilgjengelege dokument* av 9. juni 1989 nr. 32

Privatskolelova: *Lov om private skolar med rett til statstilskot* av 4. april 2003 nr. 84.

Psykisk helsevernloven: *Lov om etablering og gjennomføring av psykisk helsevern* av 2. juli 1999 nr. 62.

Sikkerhetsloven: *Lov om forebyggende sikkerhetstjeneste* av 20. mars 1998 nr. 10.

SIS-loven: *Lov om Schengen informasjonssystem (SIS)* av 16. juli 1999 nr. 66.

Straffeloven: *Almindelig borgerlig Straffelov* av 22. mai 1902 nr. 10.

Straffeprosessloven: *Lov om rettergangsmåten i straffesaker* av 22. mai 1985 nr. 25.

Strafferegistreringsloven: *Lov om strafferegistrering* av 11. juni 1971 nr. 52.

Tvisteloven: *Lov om mekling og rettergang i sivile tvister* av 17. juni 2005 nr. 90.

Åndsverkloven: *Lov om opphavsrett til åndsverk m.v.* av 12. mai 1961 nr. 2.

Forskrifter:

Abortforskriften: *Forskrift om svangerskapsavbrudd* av 14. desember 2007 nr. 1418.

Ekomforskriften: *Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste* av 16. februar 2004 nr. 401.

Forskrift om folkeregistrering av 9. september 2007 nr. 1268.

Forskrift om klinisk utprøving av legemidler til mennesker av 24. september 2003 nr. 1202.

Journalforskriften: Forskrift om pasientjournal av 21. desember 2000 nr. 1385.

Forskrift om generelle bestemmelser om utstedelse av luftfartssertifikater (BSL C 1-1a) av 20. desember 2000 nr. 1673.

Litteraturliste

ADRESSEAVISEN (2008) Du er stygg og lukter vondt, Trondheim, 2008-01-09, s. 8.

AFTENPOSTEN (2007) Vil ikke kles av på flyplassen, Oslo, 2007-11-11, s. 8.

AFTENPOSTEN.NO (2008a) *Sensitiv pasientinfo lå åpent på internett,* oppdatert: 2008-09-23, Aftenposten, (nettavis), http://www.aftenposten.no/nyheter/iriks/article2669564.ece (lest: 2008-10-10).

AFTENPOSTEN.NO (2008b) *Slakter personvernet i Norge,* oppdatert: 2008-01-10, Aftenposten, (nettavis), http://www.aftenposten.no/nyheter/iriks/article2190310.ece (lest: 2008-11-17).

AMAGASINET (2008) Fritt vilt, Oslo, 2008-02-01, s. 6.

ANDRESEN, T. (2007) Trygghet på boks, *Aftenposten,* Oslo, 2007-09-28, (debattinnlegg), s. 5.

ANGELSHAUG, T. (2008) Hva galt har Solstad sagt?, *Bergens Tidene,* Bergen, 2008-06-07, s. 44.

APENES, G. (2008) *Har personvernet noen fremtid?,* oppdatert: 2008-09-26, Digi.no, (webside), http://www.digi.no/php/art.php?id=788020 (lest: 2008-11-02).

ARNESEN, F. & SEJERSTED, F. (2008) *Datalagringsdirektivet og EØS-avtalen* (juridisk betenkning for IKT-Norge, 2008-06-06), http://ikt-norge.no/PageFiles/1555/Betenkning%20datalagring.pdf.

ARNHOLM, C. J. (1959) *Personretten*. Oslo: Tanum.

ART 29 WP (2002) *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites* (Rapport: 5035/01/EN/Final WP 56) Brussels: Article 29 data protection working party, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf.

ART 29 WP (2005a) *Data protection issues related to RFID technology* (Rapport: 10107/05/EN WP 105, 2005-01-19) Brussels: Article 29 data protection working party, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

ART 29 WP (2005b) *Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC* (Rapport: 1868/05/EN, WP 113, 2005-09-21) Brussels: Article 29 data protection working party, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_en.pdf

ART 29 WP (2006a) *Working Document 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime* (Rapport: 00195/06/EN WP 117) Brussels: Article 29 data protection working party, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf.

ART 29 WP (2006b) *Working Document on Data Protection and Privacy Implications in eCall Initiative* (Rapport: 1609/06/EN, WP 125, 2006-09-26) Brussels: Article 29 data protection working party, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf.

ART 29 WP (2007) *Opinion 4/2007 on the concept of personal data* (Rapport: 01248/07/EN WP 136, 2007-06-20) Brussels: Article 29 data protection working party, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

ART 29 WP (2008) *Working Document 1/2008 on the protection of children's personal data* (Rapport: 00483/08/EN WP 147) Brussels: Article 29 data protection working party, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf.

BAINBRIDGE, D. I. (2007) *Introduction to information technology law* (6th utgave). Harlow, England ; New York: Pearson/Longman.

BARBOSA DA SILVA, A. (Red.) (2006) *Etikk og menneskesyn i helsetjeneste og sosialt arbeid,* Gyldendal Akademisk.

BARNEOMBUDET ET AL (1999) *Barns beste i vår samtid: Et debattopplegg om begrepet barns beste i et nordisk perspektiv,* oppdatert: 1999-09-22, (PDF-document), http://www.barneombudet.no/publikasjoner/barns_best/ (lest: 2008-10-07).

BEFRING, A. K. & OHNSTAD, B. (2001) *Helsepersonelloven: Med Kommentarer* (2. utgave): Fagbokforlaget.

BERGENS TIDENE (2008) Hegnar-redaktør tar ikke ansvar, Bergen, 2008-02-22.

BERLIN, I. (1969) Two Concepts of Liberty. I BERLIN, I. (Red.) *Four Essays on Liberty*. London, Oxford University Press.

BERNT, J. F. (2008) *NAV-reformen og taushetsplikt og personvern ved omorganisering av sosial- og helsetjenestene. Foredrag på Sosial- og helsedirektoratets konferanse Fremtidsverksted for kvalitet i sosiale tjenester,* oppdatert: 2008-04-16, (Powerpoint lysbilder), http://www.shdir.no/vp/multimedia/archive/00045/Taushetsplikt_og_per_45999a.ppt (lest: 2008-10-21).

BING, J. (1991) *Personvern i faresonen*. Oslo: Cappelen.

BING, J. (2008) *Ansvar for ytringer på nett*. Oslo: Universitetsforlaget.

BJØRNSKAU, T., et al. (2007) *Security i transport og personvernets grenser* (Rapport: 914/2007) Oslo: TØI, http://pvk.no/sem080610/toi_rapport.pdf.

BLEKELI, R. D. (1977) Hva er personvern? I BLEKELI, R. D. & SELMER, K. S. (Red.) *Data og personvern*. Oslo, Universitetsforlaget, ss. 13-26.

BLEKELI, R. D. & SELMER, K. S. (1977) *Data og personvern*. Oslo: Universitetsforlaget.

BLUME, P. (1995) *Persondatabeskyttelse i den private sektor – retspolitiske overvejelser*. København: FSR.

BLUME, P. (2003) *Databeskytelsesret* (2. utgave). København: Jurist- og Økonomforbundets Forlag.

BOE, E. (1993) *Statsrett og forvaltningsrett*: Tano.

BORVIK, B. (2008a) *Personvern og ytringsfridom*, PhD-avhandling, Juridiske fakultet, Universitetet i Bergen, Bergen.

BORVIK, B. (2008b) *Utredning om det strafferettslige og sivilrettslige vernet mot ærekrenkelser*, (høringsnotat), http://www.regjeringen.no/upload/JD/Vedlegg/Hoeringer/Utredning%20om%20%C3%A6rekrenkelser.pdf.

BRATHOLM, A. (1968) Politiet og personlighetsvernet, *Lov og Rett*, s. 289ff.

BRØTEN, M. (2000) Standard for elektronisk pasientjournal, *Tobias,* vol. 9, nr. 3, ss. 18-19.

BURKERT, H. (1997) Privacy-enhancing technologies: typology, critique, vision. I AGRE, P. E. & ROTENBERG, M. (Red.) *Technology and privacy: the new landscape*. MIT Press.

BYE, R. & SJUE, F. (2008) *Overvåket*. Oslo: Gyldendal Akademisk.

BYGRAVE, L. A. (2002) *Data protection law: Approaching its rationale, logic and limits* (Information law series; v. 10). The Hague, London: Kluwer Law International.

BYGRAVE, L. A. (2003) Kryptopolitikk i en brytningstid. I GODØ, H. (Red.) *IKT etter dotcomboblen*. Gyldendal Akademisk, ss. 252–278.

BYGRAVE, L. A. (2008) *Personvernet: Lettvekter som er i ferd med å forsvinne?*, (under arbeid).

COLL, L. & LUNDE, K. (2008) Vern privatlivet!, *Dagens Næringsliv,* Oslo, 2008-01-29, (kronikk), s. 3.

CRACE, J. (2007) Walk on the wired side: jacket that lets parents keep track of children, *The Guardian,* Manchester, 2007-10-23.

DAGENS NÆRINGSLIV (2007) Norske Google skatter til Irland, Oslo, 2007-11-01, s. 60.

DAGENS NÆRINGSLIV (2008) En av fire nordmenn på Facebook, Oslo, 2008-06-11, s. 66.

DAHL, J. Y. & SÆTNAN, A. R. (2008) *«It all happened so slowly» – On controlling function creep in forensic DNA databases*, (under arbeid).

DAILY MAIL (2007) 'Safest ever' passport is not fit for purpose, London, 2007-03-05.

DANIELSSON, J., et al. (2005) *Elektroniske spor* (Rapport: 1008, 2005-06-06) Oslo: Norsk Regnesentral.

DATATILSYNET (2004) *Barn og unges personopplysninger: Retningslinjer for innhenting og bruk* (veiledning) Oslo: Datatilsynet og forbrukerombudet, http://www.datatilsynet.no/templates/article____892.aspx.

DATATILSYNET (2006) *Personvernrapporten 2006 – Retten til å være i fred* (PDF-dokument), http://www.datatilsynet.no/templates/Page____1428.aspx.

DATATILSYNET (2007a) *Høringsuttalelse – Tiltak mot trygdemisbruk mv,* oppdatert: 2007-10-15, Datatilsynet, (PDF-dokument), 07/01096-2 / SVE, http://www.datatilsynet.no/upload/hoering/2007/tiltak%20mot%20trygdemisbruk.pdf (lest: 2008-10-24).

DATATILSYNET (2007b) *Innsyn i pasientjournaler – tilgang til logg – behov for lovendring,* oppdatert: 2007-10-01, Datatilsynet, (PDF-dokument), 07/01465-1 /SVE, http://www.datatilsynet.no/upload/Dokumenter/saker/2007/07-01465-1%20Innsyn%20i%20pasientjournaler%20-%20tilgang%20til%20logg%20-%20behov%20for%20lovendring%20431994.pdf (lest: 2008-10-24).

DATATILSYNET (2008a) *Avdelinger og ansatte*, (webside), http://www.datatilsynet.no/templates/Page____904.aspx (lest: 2008-11-01).

DATATILSYNET (2008b) *Om Datatilsynet*, (webside), http://www.datatilsynet.no/templates/AboutPage____220.aspx (lest: 2008-10-05).

DATATILSYNET (2008c) *Personvernrapporten 2008 – Hva er vi redde for?* (PDF-dokument), http://www.datatilsynet.no/templates/Page____2253.aspx.

DATATILSYNET (2008d) *Uønsket informasjon om deg på nett?,* oppdatert: 2008-05-29, Datatilsynet, (webside), http://www.datatilsynet.no/templates/article____880.aspx (lest: 2008-09-11).

DATATILSYNET (2008e) *Årsmelding 2007* (PDF-dokument) Oslo, DATATILSYNET, http://www.datatilsynet.no/templates/Page____2224.aspx.

DEN NASJONALE FORSKNINGSETISKE KOMITÉ FOR MEDISIN (1993) *Registrering, bruk og gjenbruk av genetiske data* Oslo: Norges forskningsråd.

DESROSIÈRES, A. (2002) *The politics of large numbers: a history of statistical reasoning* (oversetter: NAISH, C.). Cambridge, Mass.: Harvard University Press.

DIGI.NO (2008) *PST mener Facebook er et godt verktøy,* oppdatert: 2008-11-13, (nettavis), http://www.digi.no/php/art.php?id=794163 (lest: 2008-11-18).

ECONOMIST (2003) Prepare to be scanned, 2003-12-04.

EFF (2008) *Best Practices for Online Service Providers*, (white paper), http://www.eff.org/wp/osp (lest: 2008-09-11).

EGGEN, K. (2002) *Ytringsfrihet: Vernet om ytringsfriheten i norsk rett*: Cappelen Akademisk Forlag.

ENGLEHARDT, H. T. J. (2000) Privacy and Limited Democracy: The Moral Centrality of Persons, *Social Philosophy & Policy,* vol. 17, nr. 2, ss. 120-121.

EUROPA-KOMMISJONEN (2008) *eCall – saving lives through in-vehicle electronic communication,* oppdatert: juni 2008, (PDF), http://ec.europa.eu/information_society/doc/factsheets/049-ecall-en.pdf (lest: 2008-11-12).

EUROPA-PARLAMENTET (2008) *Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection* (Rapport: P6_TA-PROV(2008)0521), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0521+0+DOC+XML+V0//EN&language=EN.

FAD (2006) *Forslag til regler om arbeidsgivers adgang til ansattes e-post mv. Endring av personopplysningsloven, nytt kapittel i personopplysningsforskriften og ny bestemmelse i arbeidsmiljøloven,* oppdatert: 2006-10-17, Fornyings- og adminsitrasjonsdepartementet, http://www.regjeringen.no/nb/dep/fad/dok/Horinger/Horingsdokumenter/2006/Forslag-til-regler-om-arbeidsgivers-adgang-til-ansattes-e-post-mv.html (lest: 2008-11-20).

FAD (2007) *Veileder i utredningsarbeid* (veiledning) Oslo: Fornyings- og administrasjonsdepartementet, http://www.regjeringen.no/nb/dep/fad/dok/Veiledninger_og_brosjyrer/2007/Veileder-i-utredningsarbeid-2.html?id=446164.

FAUCHALD, O. K. (2004) Miljøombud i naturmangfoldloven. I BACKER, I. L. (Red.) *NOU 2004:28 – Lov om bevaring av natur, landskap og biologisk mangfold*. Statens forvaltningstjeneste Informasjonsforvaltning.

FLEISCHER, P., HORVATH, J. & WHITTEN, A. (2008) *Another step to protect user privacy,* oppdatert: 2008-09-08, Google, (blog), http://googleblog.blogspot.com/2008/09/another-step-to-protect-user-privacy.html (lest: 2008-09-11).

FLØISBONN, R. (2008) Datalagring viktig for personvern, *Aftenposten,* Oslo, 2008-02-23, (kronikk), del 2, s. 5.

FOUCAULT, M. (1977) *Det moderne fengsels historie* (oversetter: ØSTERBERG, D., Fakkel nr. 370). Oslo: Gyldendal.

FOX, R. (2001) Someone to Watch Over Us: Back to the Panopticon?, *Criminology and Criminal Justice,* vol. 1, nr. 3, ss. 251-276.

GARFINKEL, S. (2000) *Software that can spy on you,* oppdatert: 2000-06-15, Salon.com, (nettavis), http://www.salon.com/tech/col/garf/2000/06/15/brodcast/index.html (lest: 2000-06-16).

GRIMSTAD, C.-E. (2008) *Privatlivets ufred: Når ord og bilder krenker*: IJ-forlaget.

GULBRANSEN, E. (1994) *Juridisk leksikon* (8. utgave). Oslo: Kunnskapsforlaget.

GAARDER, P. K. (1845) *Fortolkning over Grundloven og de øvrige Love, som danne Norges Riges offentlige Ret*. Kristiania.

HABERMAS, J. (1992) Further Reflections of the Public Sphere. I CALHOUN, C. J. (Red.) *Habermas and the Public Sphere*. Cambridge, Massachusetts and London England, The MIT Press.

HANNEMYR, G. (2002) Foucault i kyberrommet. Forbrukerrettigheter og teknologiske sperrer i vår digitale hverdag. I SLAATTA, T. (Red.) *Digital Makt*. Oslo, Gyldendal Akademisk, ss. 41-63.

HANNEMYR, G. (2005) *Hva er Internett*: Universitetsforlaget.

HANNEMYR, G. (2008a) Du kan stoppe Storebror, *Aftenposten Morgen,* Oslo, 2008-10-06, (kronikk), del 2, s. 4.

HANNEMYR, G. (2008b) Feil Nummerbruk, *Lov & Data*, nr. 92, ss. 29-30.

HANNEMYR, G. (2008c) Gull-Google skapt i garasjen, *VG,* Oslo, 2008-09-06, ss. 46-47.

HELSETILSYNET (2005) Taushetsplikten – regelverk, *Tilsynsinfo,* vol. 13, nr. 3, ss. 1-5.

HELTEN, F. & FISCHER, B. (2004) *What people think about CCTV in Berlin*, http://www.urbaneye.net/results/ue_wp13.pdf.

HES, R. & BORKING, J. (1995) *Privacy-enhancing technologies: the path to anonymity (Vols I & II)* Registratiekamer.

HILEY, D. R. (2006) *Doubt and the demands of democratic citizenship*. Cambridge ; New York: Cambridge University Press.

HINDUJA, S. & PATCHIN, J. W. (2008) *Bullying beyond the schoolyard: preventing and responding to cyberbullying*. Thousand Oaks, Calif.: Corwin Press.

HOLST, C. (2002) Retten til privatliv – En feministisk presisering med et kritisk blikk på ytringskommisjonens rapport. I HOLST, C. (Red.) *Kjønnsrettferdighet – Utfordringer for feministisk politikk*. Oslo, Gyldendal Akademisk.

ILO (1997) *Protection of workers' personal data: an ILO code of practice* Geneva: International Labour Office, http://www.ilo.org/public/english/protection/condtrav/pdf/wc-code-97.pdf.

INTEGRITETSSKYDDSKOMMITTÉN (2007) *Skyddet för den personliga integriteten. Kartlägging och analys. Del 1* (Rapport: SOU 2007:22) Stockholm: Statens Offentlige Utredningar.

JACOBS, F. G. & WHITE, R. C. A. (2006) *The European Convention on Human Rights* (4th utgave). Oxford: Oxford University Press.

JARBEKK, E. I. E. (2008) Datalagringsdirektiv – mer enn et spørsmål om lagringstid, *Lov&Data*, nr. 93, ss. 4-5.

JONGERS, M. (2006) *Retten til eget bilde: En redegjørelse, vurdering og sammenligning av den avbildedes rettsvern etter åndsverkloven § 45c, straffeloven § 390 og personopplysningsloven* (Rapport: Complex 5/06) Oslo: Senter for rettsinformatikk, TANO.

JUNGKVIST, K. (2002) Minskad möjlighet att skapa opinion, *Aftonbladet,* Stockholm, 2002-03-08.

KJØNSTAD, A. (2007) *Helserett*: Gyldendal Akademisk.

LAVIK, T. & FJØRTOFT, K. (2008) *Filosofi for samfunnsvitere*. Oslo: Universitetsforlaget.

LOMELL, H. M. (2005) Videoovervåking og menneskerettigheter, *Nordisk Tidsskrift for Menneskerettigheter*, nr. 1, s. 32ff.

LOMELL, H. M. (2007) *Selektive øyeblikk. En studie i videoovervåkningspraksis*. Oslo: Universitetsforlaget.

LYNNE, A. (2007) *Erfaringer knyttet til IPLOS. En studie blant utvalgte kommuner – bydel* TNS Gallup Institutt AS, http://www.shdir.no/vp/multimedia/archive/00052/Erfaringer_knyttet_t_52379a.pdf.

LYNNE, A. & VOLDSUND, K. (2007) *IPLOS – fra et brukerperspektiv. En studie blant to utvalgte kommuner* TNS Gallup Institutt AS, http://www.shdir.no/vp/multimedia/archive/00052/IPLOS___fra_et_bruke_52369a.pdf.

MCQUAIL, D. (2000) *Mc Quail's Mass Communication Theory* (4th utgave). London: Sage Publications.

MEDIETILSYNET (2008) *Trygg bruk-undersøkelsen 2008. En kartlegging av 8-18-åringers bruk av digitale medier* (april) Fredrikstad: Medietilsynet, MEDIETILSYNET.

MICHAEL, M. G. & MICHAEL, K. (2007) A Note on Überveillance: From Dataveillance to Überveillance and the Realpolitik of the Transparent Society. *The Second Workshop on Social Implications of National Security.* Wollongong, Australia.

MILL, J. S. (1991) *On liberty and other essays*. Oxford: Oxford university press, (opprinnelig utgave: 1859).

MAARTMANN-MOE, E. (1991) *Multimedia*. Oslo: Universitetsforlaget.

NISSENBAUM, H. (1998) Protecting Privacy in a Information Age: The Problem of Privacy in Public, *Law and Philosophy,* vol. 17, nr. 5/6, ss. 559-596.

NTB (2008) *Nemnd for fildeling,* oppdatert: 2008-07-29, E24.no, (nettavis), http://e24.no/naeringsliv/article2565245.ece (lest: 2008-09-23).

NYSTADNES, T. (2005) *Rapportserie om EPJ* (Rapport: 05/04-10) Trondheim: KITH, http://www.kith.no/templates/kith_WebPage____593.aspx.

O'REILLY, T. (2005) *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, O'Reilly Media, Inc., (web page), http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html (lest: 2008-09-07).

OMBUDSMAN (2008) Fra: *Encyclopædia Britannica Online*, http://www.britannica.com/EBchecked/topic/428288/ombudsman (lest: 2008-10-05).

OMDAHL, J. (2008) Farvel til kildevernet?, *Dagbladet,* Oslo, 2008-01-16, (kronikk).

PETRONIO, S. S. (Red.) (2000) *Balancing the secrets of private disclosures,* Lawrence Erlbaum Associates, Mahwah, N.J.

PRESTEGÅRDEN, H. (2008) Frykter misbruk av barnehagebilder, *Dagsavisen,* Oslo, 2008-03-10.

PRIVACY INTERNATIONAL (2007) *The 2007 International Privacy Ranking,* oppdatert: 2007-12-28, (webside), http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597 (lest: 2008-11-17).

RACHELS, J. (1975) Why privacy is Important, *Philosophy and Public Affairs,* vol. 4, nr. 4, ss. 323-333.

RASMUSSEN, Ø. (1997) *Kommunikasjonsrett og taushetsplikt i helsevesenet*: eget forlag.

RAVLUM, I.-A. (2005a) *Behandling av personopplysninger i norske virksomheter. En spørreundersøkelse om personvern og personopplysningsloven* (Rapport: 800/2005) Oslo: TØI, http://www.toi.no/article18652-8.html.

RAVLUM, I.-A. (2005b) *Setter vår lit til Storebror . og alle småbrødre med?* (Rapport: 789/2005) TØI, TØI, http://www.toi.no/getfile.php/Publikasjoner/T%D8I%20rapporter/2005/789-2005/789-2005.pdf.

RAWLS, J. (1999) The Idea of Public Reason Revisited. I FREEMAN, S. R. (Red.) *John Rawls: Collected Papers*. Cambridge, Cambridge University Press.

RFIDJOURNAL (2007) *Alzheimer's Care Center to Carry Out VeriChip Pilot,* oppdatert: 2007-05-25, (nettavis), http://www.rfidjournal.com/article/view/3340/ (lest: 2008-11-19).

RØHNEBÆK, Ø. (2002) Ytringsfrihet på internett. I KNUTS, G. (Red.) *Förhandlingarna vid det 36 nordiska juristmötet i Helsingfors 15-17. augusti 2002.* Helsingfors, De nordiske Juristmøder, 15-17. augusti 2002.

SAMFERDSELSDEPARTEMENTET (2002) *Fra A til B . Bedre, tryggere og mer effektiv transport – med IKT* (Rapport: N-0526), http://www.regjeringen.no/upload/kilde/sd/bro/2002/0005/ddd/pdfv/149264-ikt_i_transportsektoren.pdf.

SAMUELSEN, E. (1972) *Statlige databanker og personlighetsvern*. Oslo: Universitetsforlaget.

SAMUELSON, P. (2000) Privacy As Intellectual Property?, *Stanford Law Review,* vol. 52, nr. 5, s. 1125.

SANDEL, M. J. (1996) *Democracy's discontent : America in search of a public philosophy*. Cambridge, Mass: Belknap Press of Harvard University Press.

SCHARTUM, D. W. (1993) Mot et helhetlig perspektiv på publikumsinteresser i offentlig forvaltning? Rettssikkerhet, personvern og service, *Retfærd,* vol. 16, ss. 43-59.

SCHARTUM, D. W. (2007) *Personvern og transportsikkerhet. Personvernmessige spørsmål knyttet til tiltak for å sikre transportmidler mot fiendtlige anslag* (Rapport: CompLex 3/07) Oslo: Senter for rettsinformatikk, TANO.

SCHARTUM, D. W. & BYGRAVE, L. A. (2004) *Personvernet i informasjonssamfunnet. En innføring i vern av personopplysninger*. Bergen: Fagbokforlaget.

SCHARTUM, D. W. & BYGRAVE, L. A. (2006) *Utredning om behov for endringer i personopplysningsloven* (rapport) Oslo: Justis- og politidepartementet.

SCIENTIFIC AMERICAN (2008) Privacy In an Age of Terabytes and Terror, September 2008.

SELLEVOLD, T. & SUNDSDAL, S. (2007) *Vil overvåke skoleelever,* oppdatert: 2007-10-24, NRK, (nettavis), http://nrk.no/nyheter/distrikt/sorlandet/1.3835802 (lest: 2008-10-08).

SELMER, K. S. (1955) Bør vi få rettsregler om personlighetens rettsvern?, *Nordiskt Immateriellt Rättskydd,* vol. 24, s. 1ff.

SELMER, K. S. (1992) Oversikt over personregisterloven og Datatilsynets arbeid, *Hefte for kritisk juss*, nr. 4.

SELMER, K. S. (1996) Personvern og pasientvern. I RUYTER, K. & STORVIK, H. (Red.) *Oppsøkende genetisk veiledning*. Oslo, De nasjonale forskningsetiske komitéer.

SENNETTT, R. (1992) *Intimitetstyranniet* (oversetter: TJØNNELAND, E., Cappelens upopulære skrifter). Oslo: Cappelen forlag A/S.

SKATTEETATEN (2004) *Retningslinjer for offentliggjøring av skattelister på skatteetaten.no,* oppdatert: 2004-10-04, (webside), http://www.skatteetaten.no/Templates/Lov.aspx?id=10036 (lest: 2008-11-21).

SKOG, B. (2008) *Fra World of Warcraft til YouTube. Bruk av dataspill og nettsamfunn blant deltagere på The Gathering, 19.-23. mars 2008* Tronheim: NTNU, http://www.svt.ntnu.no/iss/Berit.Skog/rapporter/Fra%20World%20of%20Warcraft%20til%20YouTube%20Rapport.pdf.

SLETTEMARK, G. (2006) Hele folket under mistanke, *Aftenposten,* Oslo, 2006-11-15, (kronikk).

SMITH, L. & LØDRUP, P. (2006) *Barn og foreldre*. Oslo: Gyldendal akademisk.

SOLHEIM, E. (2008) *Thoughts on BitTorrent distribution for a public broadcaster,* oppdatert: 2008-03-02, NRK, (blog), http://nrkbeta.no/thoughts-on-bittorrent-distribution-for-a-public-broadcaster/ (lest: 2008-08-15).

SOLSTAD, D. (2008) Om ytringsfriheten, *Samtiden,* vol. 119, nr. 2.

SOPHOS (2007) *Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves,* oppdatert: 2007-07-14, Sophos, (web page), http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html (lest: 2008-09-12).

SOSIAL- OG HELSEDIREKTORATET (2000) *Individbasert pleie- og omsorgsstatistikk (IPLOS) i KOSTRA (kommune stat rapporteringen). Forslag til informasjonssystem for pleie- og omsorgstjenesten* (februar), http://www.shdir.no/vp/multimedia/archive/00011/IPLOS-rapporten_2000_11206a.doc.

SOSIAL- OG HELSEDIREKTORATET (2003) *Fra Tro til Kunnskap. Veileder i bruk av IPLOS sumrapporter*, http://www.shdir.no/vp/multimedia/archive/00007/IS-1113_7965a.pdf.

SOSIAL- OG HELSEDIREKTORATET (2005a) *Om IPLOS,* oppdatert: 2008-11-03, Heldirektoratet, (webside), http://www.shdir.no/iplos/om_iplos_17710.

SOSIAL- OG HELSEDIREKTORATET (2005b) *Rapport fra prosjekt. Samlemål for funksjonsvariablene i IPLOS*, http://www.shdir.no/vp/multimedia/archive/00011/Samlem_l_for_funksjo_11094a.doc.

SOSIAL- OG HELSEDIREKTORATET (2007) *IPLOS – Læringsprosess. Evaluering av beslutnings- og gjennomføringsprosessen*, HELSEDIREKTORATET, S.-O., http://www.shdir.no/vp/multimedia/archive/00052/IPLOS_-_Sluttrapport_52929a.pdf.

SOSIAL- OG HELSEDIREKTORATET (2008) *Utredning om enkel og trygg tilgjengelighet til pasientopplysninger i elektronisk pasientjournal ved ytelse av helsehjelp (EPJ) – vurdering av lovendringer* (31. mars 2008) Divisjon for spesialisthelsetjenester Sosial- og helsedirektoratet, http://www.shdir.no/vp/multimedia/archive/00043/Utredning_om_elektro_43629a.pdf.

SUNDE, I.-M. (2000) IKT-kriminalitet: Etterforskningsmetoder og personvern, *Nordisk Tidsskrift for Kriminalvidenskab*, nr. september.

SUNDE, I. M. (2008) *Beskyttelsen mot overvåking i den fysiske og elektroniske verden*, (under publisering).

SÆTNAN, A. R., YTTRI, D. J. & LOMELL, H. M. (2004) *Public opinion on CCTV in the Norwegian capital Oslo*, http://www.urbaneye.net/results/ue_wp12.pdf.

TEKNOFIL (2008) *Ytringsfriheten overgår ikke alt,* oppdatert: 2008-02-25, Mediehuset Digital AS, (nettavis), http://www.teknofil.no/wip4/ytringsfriheten_overgaar_alt/d.epl?id=25769 (lest: 2008-08-20).

TEKNOLOGIRÅDET (2004) *Holdninger til personvern. Rapport fra fokusgrupper om elektroniske spor og personvern* (Rapport: 1, februar) Oslo: Teknologirådet.

TEKNOLOGIRÅDET (2007a) *Ein ny personvernpolitikk,* 2007-11-17, (Nyhetsbrev), Oslo.

TEKNOLOGIRÅDET (2007b) *Europeiske holdninger til sikkerhetsteknologier og personvern. Rapport fra borgermøter i seks europeiske land* (Rapport: Prise 3, oktober) Oslo: Teknologirådet, TEKNOLOGIRÅDET.

TEKNOLOGIRÅDET (2007c) *Nordmenn positive til å bli overvåket,* oppdatert: 2007-06-06, (webpage), http://www.teknologiradet.no/FullStory.aspx?m=120&amid=3673 (lest: 2008-11-26).

THE AGE (2008) *Europe shelves airport full body scans,* oppdatert: 2008-11-21, (nettavis), http://www.theage.com.au/travel/europe-shelves-airport-full-body-scans-20081121-6d70.html (lest: 2008-11-21).

TOCQUEVILLE, A. D. (2003) *Democracy in America*: Penguin Classics, (opprinnelig utgave: 1835).

TRANSPORTBEDRIFTENES LANDSFORENING (2005) *Stort flertall for overvåkning,* oppdatert: 2005-01-17, (webside), http://www.transport.no/default.asp?V_ITEM_ID=2867 (lest: 2008-11-27).

TØNDEL, G. (under utgivelse) Administrating Disability: The Case of «Assistance Need» Registration in Norwegian Health and Care Governance, *ALTER. European Journal of Disability Research*.

VG (1992) Kynisk medie-bruker, Oslo, 1992-06-17, s. 10.

VGNETT (2004) *Rodney glad for seier over Se og Hør,* oppdatert: 2004-11-26, Verdens Gang, (nettavis), http://www.vg.no/rampelys/artikkel.php?artid=256196 (lest: 2008-09-23).

VGNETT (2005) *Falt om etter blind vold,* oppdatert: 2005-01-14, (nettavis), http://www.vg.no/nyheter/innenriks/artikkel.php?artid=102314 (lest: 2008-11-21).

VGNETT (2007) *Datatilsynet slakter Facebook,* oppdatert: 2007-12-05, Verdens Gang, (nettavis), http://www.vg.no/teknologi/artikkel.php?artid=187916 (lest: 2008-09-14).

VON KOSKULL, A. (1996) Personvärn och personalrekrytering, eller transformation och skygglappar, *Tidskrift utgiven av Juridiska Föreningen i Finland*, nr. 6, ss. 391–433.

WALL STREET JOURNAL (2008) NSA's Domestic Spying Grows As Agency Sweeps Up Data, 2008-03-10, del A, s. 1.

WIESE, A. (2007) Midt i debatten, *Dagbladet,* Oslo, 2007-12-18, s. 40.

WILLIAMS, C. (2007) *Schoolkid chipping trial «a success»,* oppdatert: 2007-10-22, The Register, (nettavis), http://www.theregister.co.uk/2007/10/22/kid_chipping_doncaster_go/ (lest: 2008-10-08).

WILLIAMS, R. & JOHNSON, P. (2004) Circuits of Surveillance, *Surveillance and Society,* vol. 2, nr. 1, ss. 1-14.

WORLDNETDAILY.COM (2006) *Employees get microchip implants,* oppdatert: 2006-02-10, (nettavis), http://www.wnd.com/news/article.asp?ARTICLE_ID=48760 (lest: 2008-11-17).

AANENSEN, L. T. (2007) *ID-tyveri,* oppdatert: 2007-06-15, Datatilsynet, (webside), http://www.datatilsynet.no/templates/article____1891.aspx (lest: 2009-11-18).

AAS-HANSEN, S. (2007) *På nett med barna? Et hefte om barn og unges internettbruk* (hefte, Rapport: 01/2007) Redd Barna, BARNA, R., http://www.reddbarna.no/default.asp?HMFILE=82488.

Vedlegg 1

Uttalelse om datalagringsdirektivet

Personvernkommisjonen Juni 2008

Personvernkommisjonen har drøftet EU-direktiv 2006/24 (datalagringsdirektivet) og samlet seg om en felles uttalelse. Da forslag til innføring av direktivet i norsk rett ennå ikke er lagt frem, er våre kommentarer basert på direktivteksten.

Personvernkommisjonen har som mandat å vurdere hvordan personvernet bør ivaretas i møte med motstående hensyn og verdier. Personvernkommisjonen mener det må foretas en grundig utredning av konsekvensene for personvernet dersom direktivet blir iverksatt. Vi må også få en vurdering av konsekvensene dersom direktivet *ikke* innføres i Norge.

Vi kan ikke støtte innføring av direktivet uten at *behovet* for utvidet lagring er bedre dokumentert. Både politiets og andre nasjonale myndigheters behov for utvidet lagring og tilgang til trafikkdata i det omfang som er foreslått må derfor begrunnes bedre.

Direktivets overordnede formål er å bekjempe alvorlig kriminalitet. Den teknologiske utvikling har forandret metodene som brukes både ved terror og andre former for kriminalitet. Dette har skapt et behov for nye metoder ved etterforskning og bekjempelse av kriminalitet. I fotsporene til den teknologiske utviklingen følger kriminelle som søker å utnytte denne til terrorisme og andre forbrytelser. Derfor er det viktig for politi og påtalemyndigheter å ha tilgang til de verktøyene man til en hver tid trenger til bekjempelse av kriminalitet. Det er også viktig at dette skjer innenfor demokratiske og klare rammer. Vi utelukker ikke at trafikkdata kan være viktige for politiet ved etterforskning og oppklaring av kriminelle handlinger, men vi stiller oss likevel kritisk til beslutningsgrunnlaget for den omfattende lagringsplikten som følger av direktivet. Derfor etterlyser kommisjonen dokumentasjon av politiets og andre myndigheters behov for trafikkdata i det omfang som følger av direktivet.

Personvernkommisjonen ser behovet for et regelverk både for lagring og utlevering av trafikkdata. I dag får politiet tilgang til trafikkdata fordi teletilbydere lagrer opplysningene for kommunikasjons- og faktureringsformål. Politiets tilgang til opplysninger er regulert i ulike regler og gjennom praksis fra Post- og teletilsynet. Regelverket er uoversiktlig og vanskelig tilgjengelig for borgerne. Dette er i seg selv en svakhet. Videre ser man nå en utvikling i teleoperatørenes faktureringsrutiner som kan føre til at politiet mister denne tilgangen til trafikkdata som de til nå har hatt. Som en følge av den teknologiske utviklingen går teletilbyderne fra å fakturere for *bruk* (som fordrer lagring av trafikkdata) til å fakturere for *tilgang*. Dermed har de ikke behov for å lagre trafikkdata. En slik utvikling gjør at politiet vil miste verdifull informasjon. Etter Personvernkommisjonens oppfatning er det derfor ønskelig med en *grundig utredning av behovet for et regelverk som sikrer politiets arbeidsmetoder og ivaretar personvernet*.

I enkelte saker er det vanskelig for politiet å få tak i vitner. Tendensen er særlig tydelig innen organisert kriminalitet. I slike saker ser man at trafikkdata og elektroniske spor er svært sentrale bevis. Informasjonen er på mange måter et taust vitne og representerer i mange saker en tråd som lar seg følge. Men dersom det legges opp til pliktig lagring av trafikkdata, så vil det sannsynligvis forekomme ønsker/press fra ulike hold for å få tilgang til disse data.

Kredittilsynet og tollvesenet kan finne gode begrunnelser for at tilgang til trafikkdata vil bistå disse etatene i sitt arbeid. Helsevesenet kan argumentere for at kartlegging av sosiale kontaktnett gjennom trafikkdata kan redde liv og helse når man trenger å spore bærere av alvorlige smittsomme sykdommer. Nød- og redningsetater vil kunne argumentere for at trafikkdata vil kunne hjelpe dem med sporing av savnede personer. Personvernkommisjonen mener det er en reell fare for at pliktmessig lagring av trafikkdata med bekjempelse av alvorlig kriminalitet som formål etter hvert vil resultere i at disse data bru-

kes til andre formål[1], som hver i sær kan være gode, men hvor den samlede bruken kan utgjøre en alvorlig trussel mot personvernet.

Personvernkommisjonens fokus er naturlig nok direktivets innvirkning på personvernet. Vi mener at datalagringsdirektivet setter både personvernet og ytringsfriheten på prøve. Dette vil gjelde selv om lagring av trafikkdata i henhold til direktivet ikke anses som kontinuerlig eller regelmessig overvåkning av borgerne. Verdien av lagring må nemlig også veies opp mot effekter på frimodighet. Dette gjelder selv om formelle friheter ikke berøres, og selv om de registrerte data kun skal være tilgjengelige for politiet under regulerte forhold. Allerede vissheten av at noen *kan* lete seg fram til dine kontakter og dine bevegelser, både i det virkelige rommet og på Internett, kan være nok til å hemme borgere i utøvelsen av sine friheter til å samles, til å ytre seg og til å søke opplysninger. Dette er grunnleggende rettigheter i et demokrati, som kommer til uttrykk både i norsk lovgivning og i Den europeiske menneskerettskonvensjon (EMK). Etter kommisjonens oppfatning vil innføring av direktivet kunne svekke opplevelsen av privatliv og privat kommunikasjon.

EMK artikkel 8 annet ledd åpner for at det kan gjøres inngrep i personvernet. For at et slikt inngrep skal være forsvarlig må det blant annet være *nødvendig i et demokratisk samfunn*. I dette ligger det etter Den Europeiske Menneskerettighetsdomstolens (EMD) praksis at det må være en «pressing social need» for å gripe inn i personvernet. Det holder ikke at det er hensiktsmessig, rimelig eller ønskelig. Inngrepet som gjøres må dessuten være proporsjonalt i forhold til formålet som ønskes oppnådd. Den omfattende lagringsplikten som følger av direktivet kan etter Personvernkommisjonens oppfatning være problematisk i forhold til nødvendighetsprinsippet og proporsjonalitetsprinsippet. Forskning fra blant annet Tyskland[2] sår tvil om betydningen av trafikkdata for oppklaring av kriminalitet. Rapportene fra Tyskland omhandler selvsagt forhold knyttet til det tyske kriminalitetsbildet, og kan dermed ikke påberopes direkte i forhold til norske forhold. Kripos mener å ha erfaring for at trafikkdata har stor betydning for oppklaring av kriminalitet. Personvernkommisjonen etterlyser imidlertid en studie, tilsvarende den man har gjort i Tyskland, for norske forhold. Kriteriene som følger av EMK artikkel 8 krever etter kommisjonens oppfatning en grundig klargjøring i form av *dokumentasjon av behovet for lagring* (både lagringstid og omfanget av opplysninger) og en grundig konsekvensutredning: Både personvernmessige konsekvenser av en eventuell innføring og konsekvenser for politiet og kriminalitetsbildet dersom Norge ikke innfører direktivet. Personvernkommisjonen er usikker på om slik dokumentasjon eller utredninger ligger til grunn for direktivet eller for arbeidet som er gjort i forbindelse med en eventuell innføring av direktivet i norsk rett.

Det synes klart for Personvernkommisjonen at direktivet representerer noe nytt i forhold til dagens regime for lagring av trafikkdata. Direktivet innebærer for det første *lagring av nye typer data*, som for eksempel geolokaliseringsdata og epostlogger. For det andre vil direktivet medføre *lengre lagringstid* enn det som følger av dagens praksis. For det tredje berøres langt *flere organisasjoner* enn det som er dagens situasjon, blant annet omfatter direktivet mange ISPer. For det fjerde gir direktivet et *nytt normativt grunnlag* for lagring av trafikkdata – en plikt til å lagre for andre formål enn faktureringsformål. Det er også et moment at man går fra en *rett til å lagre opplysninger* for visse formål, til en *plikt til å lagre opplysninger*. Disse forholdene må hensyntas i vurderingen av om og eventuelt hvordan direktivet skal innføres i norsk rett.

Dersom direktivet skulle bli innført, mener kommisjonen at det er viktig at lagringstiden gjøres så kort som mulig. Personvernkommisjonen vil også peke på spørsmålet om hvilken sikkerhet man har for de opplysningene som lagres. Mye tyder på at mange organisasjoner ikke har fullgode mekanismer for sikring av trafikkdata mot uautorisert spredning.[3] Det har vært fremhevet som en

---

[1] Våren 2008 ble det rapportert at Deutsche Telekom ulovlig hadde analysert trafikkdata i et forsøk på å identifisere en pressekilde, jf. Prosecutors investigate Deutsche Telekom over data misuse; 29. mai 2008, tilgjengelig på adresse: http://www.out-law.com//default.aspx?page=9153.; Overvåkingsskandalen vokser; 3. juni 2008, tilgjengelig på adresse: http://e24.no/utenriks/article2462382.ece.

[2] Se: Max-Planck-Institut für ausländisches und internationales Strafrecht: Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO: Forschungsbericht im Auftrag des Bundesministeriums der Justiz (Freiburg, februar 2008); tilgjengelig på adresse: http://www.vorratsdatenspeicherung.de/images/mpi-gutachten.pdf, som hevder at trafikkdata kun vil bidra til oppklaring i et lite antall, anslagsvis 0,002 % av det totale antall kriminalsaker, og anslag fra det tyske Bundeskriminalamt, som ifølge en separat studie utført sommeren 2007 regner med at datalagring vil føre til en økning i oppklaringsraten «fra dagens 55 prosent, i beste fall til 55,006 prosent», jf. http://www.heise.de/newsticker/Vorratsdatenspeicherung-fuer-eine-0-006-Prozentpunkte-hoehereAufklaerungsquote–/meldung/92746.

trussel mot sikkerheten at tilbydere pålegges å lagre store mengder data på vegne av myndighetene, og at manglende egeninteresse i lagring av opplysningene til dette formålet vil kunne gå ut over sikkerheten. Dersom lagring i en så omfattende skala som direktivet legger opp til blir gjennomført, må det fra myndighetens side settes krav til sikring i form av kryptering og deponeringsmekanismer som hindrer at så vel teletilbyderen selv, som myndighetene, kan få tilgang til lagrede data før korrekt rettslig grunnlag for tilgang kan fremlegges. Det må også sikres at enhver tilgang som gis, avgrenses til de data det skal være lovlig tilgang til. Det er etter kommisjonens oppfatning avgjørende at en eventuell innføring av direktivet ledsages av sikringer – tekniske og organisatoriske så vel som juridiske – mot at det lagrede materialet kan brukes til strategisk informasjonsanalyse eller andre former for generell informasjonssøking. I forhold til den tekniske siden vil dette innebære at det må utvikles nye, finmaskede systemer for tilgangskontroll og datasikring som, så vidt Personvernkommisjonen har kjennskap til, ikke er tilgjengelig på markedet i dag.

Oslo 12. juni 2008

[3] Personvernkommisjonen viser til den såkalte Tele2-saken, hvor Tele2 våren og sommeren 2007 lot kredittopplysninger om et sekssifret antall personer tilflyte uvedkommende. En enda større skandale fant sted i Storbritannia høsten 2007, hvor to ukrypterte disker med personopplysninger vedrørende alle familier i Storbritannia med barn under 16 år kom på avveie. Se: *Brown apologises for records loss,* BBC News, 21. november 2007, http://news.bbc.co.uk/2/hi/uk_news/politics/7104945.stm.

Vedlegg 2

Nemnd for Internett

Om et mulig tvisteløsningsorgan for krenkelser på Internett

advokat Andreas Galtung Oslo, oktober 2008

1 Innledende bemerkninger

1.1 Konklusjon

Denne betenkningen konkluderer med at det bør opprettes en nemnd for lovstridige krenkelser på Internett som følger.

Nemnda bør:

- Være offentligrettslig basert.
- Statlig finansiert.
- Hjemlet i ehandelsloven av 23. mai 2003 nr 35.
- Lagt administrativt til Nærings- og handelsdepartementet, alternativt Post- og teletilsynet.
- Ha mellom fem og åtte medlemmer.
- Ha retting, sletting og stengning som sanksjon.

1.2 Mandat og bakgrunn for betenkningen

Personvernkommisjonen mener at personvernkrenkelser på Internett er et økende problem, og at dette reiser vanskelige avveininger mellom ytringsfrihet og personvern. Personvernkommisjonen har gjennom åpne møter og samtaler med fagpersoner registrert at slike saker sjelden finner veien til domstolene.

I denne sammenheng har Personvernkommisjonen ønsket å utrede hvorvidt et alternativt tvisteløsningsorgan vil kunne gi publikum et bedre tilbud i forhold til dagens situasjon. En av Personvernkommisjonens medlemmer, uttalte til Barnevakten.no at:

> «En klagenemnd vil være et lavterskeltilbud, der man rapporterer at man opplever seg krenket ved å henvise til den aktuelle nettsiden. Deretter får man en tilbakemelding fra blant andre fagjurister om det er snakk om en overtredelse av personvernet.[1][2]»

Dette dokumentet tar for seg ulike måter en slik nemnd vil kunne organiseres på for å kunne fungere praktisk. Det vil i denne sammenheng vises en del til prøveprosjektet Nettnemnda som IKT-Norge tok initiativ til i 1997, og som fungerte som prøveprosjekt fra 2001 til 2003.

Det er først og fremst de mange hendelsene om krenkelser av personvernmessig art, som i det siste har fått medias oppmerksomhet, og som har fått Personvernkommisjonen til å gå inn for å utrede opprettelsen av en klagenemnd for Internett. Dette reiser mange spørsmål. Denne rapporten tar for seg de viktigste.

Det en helt enkelt tenker seg er en nemnd som kan ta i mot klager fra personer eller organisasjoner som føler seg krenket. Nemnda skal da kunne behandle disse raskt og først og fremst sørge for at krenkelsene stoppes.

En hovedutfordring i denne sammenhengen for klagenemnda vil være å balansere hensynet til ytringsfriheten og hensynet til personvernet. Både ytringsfrihet og personvern er sentrale menneskerettigheter, som er vel grunnfestet i blant annet Den europeiske menneskerettighetskonvensjon, EMK[3].

Hovedspørsmål i forhold til etablering av en klagenemnd for Internett.

Slik jeg ser det blir de viktigste spørsmål som bør avklares følgende:

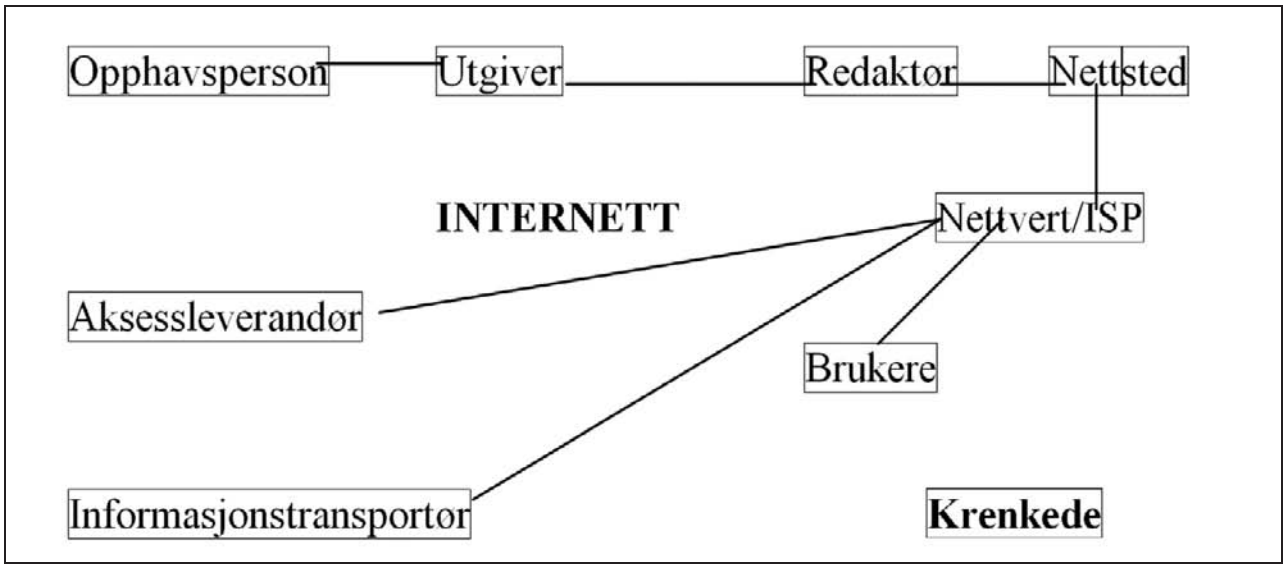
Forholdet til andre institusjoner
Hva skal mandatet til nemnda være
Rettslig grunnlag
Finansiering
Sammensetning og organisering

---

1 Gisle Hannemyr til www.barnevakten.no 4. juni 2008.

2 Det skal bemerkes at denne uttalelsen var for Hannemyrs egen regning og ingen offisiell uttalelse fra Personvernkommisjonen.

3 Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950.



Figur 2.1

1.3 Formålet med en nemnd

Bakgrunnen for at Personvernkommisjonen ønsker seg en nemnd for Internett, er de mange krenkelser som forekommer på nettet. Spørsmålet er så når en har med en Internettkrenkelse å gjøre. Svaret på det er ganske enkelt. *En har med en nettkrenkelse å gjøre i de tilfeller der personopplysninger tilgjengeliggjøres på nettet, og denne tilgjengeliggjøringen er uønsket i forhold til den personopplysningene gjelder.*

Den mest typiske form for krenkelse vil være at bilder eller tekst legges ut på en hjemmeside. Nemndas oppgave vil da først og fremst være å få krenkelsen til å opphøre. For å få til dette, vil man trenge et regelverk med et sett av sanksjoner.

2 Aktører og avtalerelasjoner

For å få en nemnd til å virke, må en ha klart for seg de viktigste aktørene på nettet. Bare på den måten vil en kunne lage et rettet regelverk. I Nettnemndas regelverk, etiske regler punkt 2, definert for Internett, benyttet en følgende definisjoner som er forholdsvis beskrivende for aktørbildet på Internett:

2.1 *Nettsted* er en samling informasjon, tilgjengelig via Internett, som fremstår som en enhet under samme ledelse.
2.2 *Opphavsperson* er den som har utformet informasjon på nettstedet.
2.3 *Redaktør* er den person som treffer avgjørelse om informasjonsinnholdet på nettstedet.
2.4 *Utgiver* er den som i henhold til avtale (med vert, aksessleverandør og/eller andre), har rett til å gjøre tilgjengelig informasjon på nettsted.
2.5 *Aksessleverandør* er den som tilbyr teknisk tilgang til Internett.
2.6 *Informasjonstransportør* er den som transporterer data på Internett.
2.7 *Vert* er den som er ansvarlig for lagring av hele eller deler av et nettsted.

En kan da få en struktur som vist i figur 2.1:

En kan nok i ulike juridiske fremstillinger og i lovgivningen finne noe forskjellig begrepsbruk, men jevnt over tror jeg denne er ganske dekkende. Begrepet opphavsperson er for eksempel meget uvanlig. Det en tenkte da var at det omfattet den som er opphav til materialet eller den som er ansvarlig for den originære ytring. Ordet nettvert synes imidlertid å ha blitt det norske ordet for ISPer (Internet Service Provider), men ordene forekommer gjerne om hverandre. Jeg holder meg til ordet nettvert som også er brukt i forarbeider til ehandelsloven og juridisk litteratur.[4]

Det som har vært det store temaet i mange saker og debatter, er hva slags ansvar nettverten skal og bør ha. Dette er det skrevet mye om, og jeg går ikke nærmere inn på dette her. Det som imidlertid er på det rene er at nettverten er den aktøren som enklest kan få et forhold til å opphøre, da det er han som enkelt kan «trekke ut pluggen». På den annen side er det nettvertens oppgave å være en teknisk

[4] Se for eksempel Jon Bing: *Ansvar for ytringer på nett*. Særlig side 231. Oslo 2008.

tilrettelegger og etter loven er det klart at ansvaret meget begrenset. Videre er det klart at nettverter i utgangspunktet ikke har noen plikt til å overvåke eller eventuelt finne ulovlig materiale.

3 Litt om prøveprosjektet Nettnemnda

Arbeidet med Nettnemnda begynte allerede i 1997 da IKT-Norge etablerte en referansegruppe med oppgave å utarbeide et regelverk for å ta seg av krenkelser på Internett.[5] I august 1998 lå et ferdig forslag på bordet. På grunn av manglende finansiering kom ikke prøveprosjektet i gang før i 2001. Nemnda ble offisielt åpnet i september 2001.

Nettnemnda var en avtalebasert nemnd basert på frivillig deltakelse og finansiert av bransjen. Den fungerte ved at de som var med ga sin tilslutning til det som ble betegnet som det Internett-etiske regelverket. Nettvertene tok i sin tid med som vilkår i sine abonnementskontrakter med kundene at de forholdt seg til det Internett-etiske regelverket.

Etter meget usikre beregninger er det antatt at ca 50-60 % av norske internettbrukere var tilknyttet nettverter som hadde akseptert Nettnemnda.

Det var selvfølgelig ikke tilfredsstillende med så mange utenfor ordningen, men det var en god begynnelse. På sikt ville en kanskje kunne få større tilslutning, særlig om nettvertene hadde sett at det kunne være en gevinst i å være tilsluttet.

I løpet av 2003 døde prosjektet. Ikke fordi behovet for ordningen ikke fantes, men fordi det ikke var vilje til å finansiere den. Det var heller aldri noe rush av saker. Det vil uansett ta noe tid før en nemnd som dette fylles opp av saker. Den må blant annet bli tilstrekkelig kjent. Dog vil det nok i dag gå mye fortere i og med at bruken av Internett er så mye større og personvernkrenkelser har fått enda mer oppmerksomhet. Professor Jon Bing har i forbindelse med Nettnemnda hevdet at: *Det behov som ordningen var tenkt å dekke, finnes fremdeles – og muligheten for å gjenoppvekke Nettnemnda eller etablere en lignende ordning, bør ikke avskrives.*[6]

[5] For en mer detaljert gjennomgang se: Andreas Galtung: *The Norwegian Internet Ethical Council* I. Scandinavian Studies In Law vol 47, s 407-419 og Andreas Galtung: *Nettnemndas grunnlag og virksomhet – et eksempel på selvregulering.* Tidsskrift for forretningsjus nr. 4 2002.

[6] Jon Bing: *Ansvar for ytringer på nett*. side 255. Oslo 2008.

4 Er det behov for en nemnd for krenkelser på Internett

Det store spørsmålet er selvfølgelig om det er et behov for en særskilt nemnd for nettkrenkelser. I forbindelse med at Personvernkommisjonen foreslo en nemnd på forsommeren skrev Dagbladet blant annet på lederplass om forslag til en nemnd:[7]

> «*Dette er en helt* usedvanlig dårlig idé. En statlig riksredaktør med egen sensurmyndighet er det aller siste vi trenger. Det er også i strid med helt grunnleggende prinsipper om hvordan ytringer reguleres i et åpent samfunn. I dag foregår det gjennom lovgivningen og ved aktiv bruk av frivillige og uavhengige institusjoner som Pressens faglige utvalg. Det er altså domstolene og mediene selv som setter grensene. En nemnd med myndighet til å stenge sider på internett uten domstolsbehandling, hører hjemme i autoritære stater. Vi håper Personvernkommisjonen ikke legger seg på et slikt nivå når det gjelder personvernet.»

I dette avsnittet har Dagbladet etter min mening misforstått forslaget. For det første kan en ikke si at det er snakk om sensur. Det er snakk om en nemnd som kan få stoppet visse former for krenkelser når disse er et faktum. Det vil heller ikke være snakk om en nemnd som kommer i stedet for domstolsbehandling. Det er selvsagt at en avgjørelse fra nemnda vil kunne bringes inn for domstolene. Det er heller ikke nødvendigvis sikkert at en nemnd bestående av for eksempel et antall kvalifiserte personer vil bety mindre rettsikkerhet enn en prosess der en avgjørelse bringes inn for en dommerfullmektig i Oslo tingrett. Det skal dertil legges til at svært mange av rettsprosessene i vårt samfunn nettopp finner sted i nemndbehandling. Dette er ikke minst tilfellet innenfor forbrukersektoren. Dette er for øvrig helt i tråd med prinsippene i den nye tvisteloven av 17. juni 2005 nr 90, om at konflikter søkes løst utenfor domstolene.

Det er for øvrig en misforståelse at en nemnd nødvendigvis vil stoppe ytringer på nettet. En kan godt tenke seg tilfeller der en nemnd vil ha den oppfatning at en ytring er lovlig, men at for eksempel en nettvert vil ønske stengning for ikke å risikere ansvar.

[7] Dagbladet 9. juni 2008. Leder.

For publikum vil en nemnd være et gode fordi man da har et sted å henvende seg. Et slikt sted finnes ikke i dag.

For deler av næringen vil en nemnd også ha store gevinster. I den sammenhengen kan en se hen til det som lå bak IKT-Norges forslag til Nettnemnda i 1998. Hovedbegrunnelsen her var at en så at nettverter hadde store utgifter til advokater for å vurdere ulovlig innhold. Kanskje søkte de ikke råd i det hele tatt, men valgte å stenge sider i stedet for å risikere et erstatningssøksmål og i verste fall straff. I slike tilfeller en det særlig nyttig å kunne ty til en nemnd som har mulighet til i de mest graverende tilfeller å beslutte stengning av en nettside. I og med at Internettutbredelsen er veldig mye større i dag enn for ti år siden, er dette argumentet minst like relevant i dag som da.

Det finnes ingen eksakt oversikt over hvor mange eller hvilke krenkelser som finner sted på Internett. Man vet at de dukker opp fra tid til annen, og det er ingen grunn til å anta at omfanget ikke er økende. Som eksempel på den type saker som kan tenkes å komme opp vil jeg her trekke frem noen av de saker som var oppe for prøveprosjektet Nettnemnda. Jeg tror de vil være typiske for den type saker som vil kunne dukke opp i en fremtidig nemnd. De er alle hentet fra Tidskrift for forretningsjuss nr 4 2002.[8]

En sak gjaldt fotografier lagt ut på nettet av et homofilt par som hadde sex. Nettnemnda kom til at dette var klart i strid med Etiske regler for Internett punkt 4.3 og henviste dessuten til at dette var i strid med åndsverklovens § 45 c, av 12. mai 1961 nr 2, om retten til eget bilde, som har det klare utgangspunkt at personfotografier ikke kan publiseres uten avbildedes samtykke, med mindre det kommer inn under noen av unntakene. Det var åpenbart at ingen av de unntakene var aktuelle her.

Et poeng i denne saken var at verten for siden ikke var tilsluttet Nettnemnda. På hjemmesiden www.gay.guide.no har en imidlertid sagt at man følger pålegg fra Nettnemnda. Dette gjorde de med en gang Nettnemnda fattet hastevedtak i saken på grunn av sakens alvorlige karakter. Således er dette et eksempel på at Nemndas vedtak fikk effekt selv om saken gjaldt aktører som ikke var forpliktet til det.

I to saker tok Nettnemnda stilling til personomtale som klager ønsket fjernet. Den første saken gjaldt en klager som henvendte seg til Nettnemnda fordi hans navn var publisert under kategorien «NS-barn» på nettsidene til en forening for norske NS-barn. Klager ville ikke være assosiert med nettstedet eller fremstå som NS-barn. Et ytterligere poeng var at klager var født i 1954. Hans foreldre hadde riktignok vært i NS, men for klager var dette en fortid han ikke selv var del av.

Nettnemnda konkluderte her med at utgiver burde endre på karakteristikken av klageren, ved at kategoriseringen av opplysningene om klagerens avisinnlegg ble endret. Nemnda uttrykte således:

> «… at det på bakgrunn av en uklar forståelse av begrepet «NS-barn», samt klagerens sterke protester mot bruken av denne betegnelsen på ham, vil være utilbørlig å karakterisere personen som «NS-barn», jf. punkt 4.3 i de nettetiske reglene. I samsvar med 6.3 i disse reglene, pålegger Nettnemnda utgiver å endre eller fjerne klassifikasjonen av intervjuet med klageren. Etter Nettnemndas syn kan personnavn og referanse beholdes, men disse opplysningene kan ikke knyttes til betegnelsen «NS-barn» eller tilsvarende betegnelse.»

Den andre saken gjaldt en klage på innhold i en privat dagbok lagt ut på en privat hjemmeside. Her ble det opplyst at klager for 25 år siden var del av et homofilt miljø. Videre ble klager nevnt i forbindelse med en person som ble antatt muligens å ha pedofile trekk. Slik Nettnemnda så det, var dette en sak der en måtte foreta en balansegang mellom hensynet til personvern og hensynet til ytringsfrihet. Nettnemnda konkluderte her med at hensynene til både personvern og ytringsfrihet kunne ivaretas ved at klager ble anonymisert. Nettnemnda uttrykker følgende:

> «Formuleringene om klageren inneholder ingen direkte påstand om seksuell legning eller avvik. Meningsinnholdet er imidlertid vagt og gir rom for mange tolkninger. Uansett om det saklige innholdet er uklart, er det videre på det rene at utsagnene gjelder klagerens seksualitet. Slike opplysninger er i lovgivningen ellers regnet som sensitive og spesielt beskyttelsesverdige, se for eksempel personopplysningsloven § 33, jf. § 2 nr 7. [lov av 14 april 2000 nr. 31]
>
> Etter Nettnemndas vurdering er det i denne saken mulig både å ta tilbørlig hensyn til klagerens personvern og innklagedes ytringsrett. Dette kan skje ved å fjerne klare personidentifiserbare kjennetegn slik at klagerens navn ikke framkommer ved søk på navnet.

[8] Andreas Galtung: *Nettnemndas grunnlag og virksomhet - et eksempel på selvregulering.* Tidsskrift for forretningsjus 2002 nr. 4 s. 524 - (TFF-2002-524).

> I medhold av punkt 6.3 i Etiske regler for Internett pålegger Nettnemnda innklagde straks å erstatte klagerens fulle navn med initialer.»

Som en ser av sakene nevnt ovenfor, er de fleste av personvernmessig karakter. En kunne tenke seg at en hadde hatt flere klager vedrørende immaterielle krenkelser, men de har imidlertid ikke kommet.

Som eksempel på et tilfelle som ikke dreide seg om personvern kan nevnes en uttalelse der en tilbyder av pornografisk materiale på Internett tok betaling for dette ved hjelp av tilleggsfakturerte SMS-meldinger. Opplegget virker slik at man ved å sende en SMS til et spesielt nummer får tilbake et passord som gir en tilgang til visse sider. Nettnemnda valgte å uttale seg om dette ut fra det synet at en mener mobilabonnenter burde ha anledning til å velge bort overfakturerte tjenester av denne typen ut fra det syn at det er en fare for at en abonnent ville kunne pådra seg uforholdsmessige store kostnader. Om dette uttalte Nettnemnda:

> «Etter Nettnemndas syn bør de aktuelle betalingstjenestene så langt som råd være basert på forhåndsavtale mellom betalingsformidler og bruker (opt-in). I alle tilfelle bør det være mulig for brukere å reservere seg mot tjenesten (opt-out).
>
> En tjeneste som ikke inneholder noen form for mekanismer som gjør det mulig å ivareta forbrukerinteresser, kan etter Nettnemndas mening vanskelig sies å være i samsvar med punkt 4.3 i de nettetiske reglene.»

I og med at Nettnemnda her bare kunne gi en veiledende uttalelse, ble den ikke fulgt opp. Det var imidlertid Nemndas tro at uttalelser av denne typen kan være nyttige innlegg i den forbrukerpolitiske debatt.

Andre tilfeller som kanskje kunne egne seg for en nemnd er de tilfeller en har sett av ulovlig fildeling og krenkelser av opphavsretten for øvrig. I Nettnemndas tid fikk man ingen slike saker, men slike saker hadde nok kommet. Ikke minst er advokatfirmaet Simonsens engasjement på vegne av Norsk Videogramforening illustrerende. Mars 2008 ba advokatfirmaet Simonsen på vegne av Norsk Videogramforening nettleverandører om å videresende en erklæring til kunder som de mente sto bak ulovlig fildeling. I erklæringen ble kundene bedt om å skrive under på og sende inn en bekreftelse om at de skulle avstå fra ulovlig fildeling i fremtiden.

Dette skjedde etter at advokatfirmaet Simonsen i 2007 hadde registrert og lagret IP-adresser hvor de registrerte uautorisert opp- og nedlasting av norske spillefilmer. Innhentingen av disse opplysningene ble gjort med konsesjon fra Datatilsynet.

Forbrukerrådet og IKT-Norge reagerte sterkt på erklæringene, som de mente satte forbrukerne i en uklar rettssituasjon, med et nærmest ubegrenset ansvar overfor rettighetshaverne. Forbrukerrådet pekte også på at de mener Internett er et nødvendighetsgode som bare unntaksvis kan fratas borgerne. Advokatfirmaet Simonsen uttalte senere i norske media at de hadde til hensikt å fremlegge erklæringene dersom det senere ble aktuelt å forfølge forbrukerne rettslig.

Situasjonen illustrerer problemene som oppstår når politi og domstoler avviser å følge opp søksmål eller anmeldelser mot fildelere, slik praksis hittil har vist seg å bli i Norge. I debatten som pågikk i 2008 var partene enige om at opphavsretten skal respekteres og at rettighetshaverne må ha muligheter til å forfølge antatte rettighetsbrudd. I mangel av uavhengige tvisteløsningsmuligheter anså rettighetshaverne at de ikke hadde annet valg enn å opptre som privat Internett-politi. Dette er meget tvilsomt. På den annen side er det opplagt at mye av den fildeling som foregår er ulovlig. I slike tilfeller vil en uavhengig nemnd opplagt kunne ha en viktig oppgave. Parter involvert i en tvist som dette vil dessuten føle det betryggende at det er en uavhengig nemnd som treffer en avgjørelse og et ikke privat advokatfirma som prøver å påtvinge forbrukere erklæringer.

5 Rettslig problemstilling og begrunnelsen for ønsket

Jeg har ovenfor gitt eksempler på typetilfellene som begrunner ønsket om et tvisteløsningsorgan. Går en ti år tilbake i tid, kunne en stadig lese at på Internett er det fullstendig anarki og lover og regler gjelder ikke. Denne misforståelsen eksisterer i langt mindre grad i dag. Saken er den at de regler som ellers gjelder stort sett gjelder i forhold til Internett også. Det som på den annen side er helt klart er at antallet nettkrenkelser forekommer i større grad enn tidligere, noe som skyldes den nesten totale utbredelse av Internett og at opplasting stadig blir enklere. Et moment til kan være utbredelsen av kameramobilen. *Alle* har i dag mobiltelefon og nesten alle telefoner er utstyrt med kamera. Det innebærer at det er langt

flere som går med kamera på seg til enhver tid i forhold til tidligere.

Det rettslige utgangspunkt for diskusjonen er at krenkelser forekommer og dermed også lovbrudd. På den annen side er ytringsfriheten beskyttet. Den store utfordringen er å finne et system som kan gjøre disse rettigheter til en realitet.

5.1 Ytringsfriheten som et utgangspunkt

En kan godt si at som en overordnet grunnregel er informasjon tilgjengeliggjort på nettet beskyttet av ytringsfrihet nedfelt i Grunnlovens § 100 og ikke minst EMK artikkel 10:

> *«Art 10. Ytringsfrihet*
>
> 1. Enhver har rett til ytringsfrihet. Denne rett skal omfatte frihet til å ha meninger og til å motta og meddele opplysninger og ideer uten inngrep av offentlig myndighet og uten hensyn til grenser. Denne artikkel skal ikke hindre stater fra å kreve lisensiering av kringkasting, fjernsyn eller kinoforetak.
>
> 2. Fordi utøvelsen av disse friheter medfører plikter og ansvar, kan den bli undergitt slike formregler, vilkår, innskrenkninger eller straffer som er foreskrevet ved lov og som er nødvendige i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, territoriale integritet eller offentlige trygghet, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, for å verne andres omdømme eller rettigheter, for å forebygge at fortrolige opplysninger blir røpet, eller for å bevare domstolenes autoritet og upartiskhet.»

Grunnloven § 100 og EMK artikkel 10 gir både sterke uttrykk for ytringsfriheten, men også for at det kan gjelde begrensinger i eller unntak fra den. De må være nødvendige og forholdsmessige.

5.2 Nettkrenkelser

Om en sier at ytringsfriheten er et utgangspunkt så har denne mange unntak. Jeg tror en kan dele internettkrenkelser inn i tre grove hovedkategorier:

1. Personvern- og omdømme og integritetskrenkelser (dette er krenkelser som retter seg inn mot enkeltpersoner eller grupper av personer). Utvidet omfatter dette reglene i personopplysningsloven, injuriereglene, beskyttelsen av privatlivets fred og det ulovfestede personvern.
2. Immaterialrettslige krenkelser. Dette er særlig brudd på åndsverklovens regler om opphavsmannens enerett.
3. Skadelig og harmfullt materiale. Typisk eksempel er ulovlig barnepornografi, skadeverk, oppfordring til ulovligheter og ulovlig oppfordring til selvmord.

Jeg går nedenunder overfladisk gjennom ulike eksempler på typer av krenkelser. For en mer grundig behandling kan det henvises til Jon Bings *Ansvar for ytringer på nett*.[9] Det som en imidlertid må vurdere, er om en nemnd bør ta for seg alle nevnte typer eller bare begrense seg til de rene personvernkrenkelser.

5.3 Personvernkrenkelser

Overordnet er det snakk om EMK artikkel 8 som lyder:

> *«Art 8. Retten til respekt for privatliv og familieliv*
>
> 1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.
>
> 2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.»

I svært mange spørsmål om nettkrenkelser vil en måtte ta disse to bestemmelsene i betraktning. Andre relevante bestemmelser vil kunne være:

Vernet om privatlivets fred i straffeloven av 22. mai 1902 nr. 10 § 390, vernet om retten til eget bilde i åndsverklovens § 45 c, straffelovens injuriebestemmelser, jf. straffelovens §§ 246-247 og selvsagt personopplysningsloven. Også ansvar for rasistiske ytringer kan en ta med her, jf. straffelovens § 135a.

I tillegg kan en nevne et uttall av bestemmelser angående taushetsplikt spredt rundt i lovgivningen som meget lett kan bli aktuelle i forbindelse med nettkrenkelser.

Når Personvernkommisjonen har engasjert seg, er det fordi krenkelser av personvernmessig art lett kan forekomme på nettet, og at en har sett at publikum ofte ikke har andre muligheter enn å

---

[9] Jon Bing: *Ansvar for ytringer på nett*. Særlig side 33-78. Oslo 2008.

henvende seg til advokat eller politi med spørsmål om krenkelsene skulle ansees straffbare. Med mindre det virkelig dreier seg om veldig alvorlige tilfeller, vil politiet mest sannsynlig henlegge slike saker, mens de sivilrettslige vil koste så mye at de færreste vil orke eller makte å forfølge dem.

5.4 Immaterialrettslige krenkelser og likeartede krenkelser

Når det gjelder internettkrenkelser av immaterialrettslig art som for eksempel ulovlig fildeling av musikk vil det her som regel dreie seg om brudd på åndsverklovens § 2. Disse blir ofte forfulgt av musikkprodusentenes organisasjoner, som har råd til å betale advokater til å forfølge saken.

Problemstillinger rundt dette vil kunne ha sider til personvernet, for eksempel rundt eventuelle rettigheter og plikter til identifikasjon av dem som begår overtredelsene. Det i seg selv kan være et argument for at slike krenkelser bør tillegges en eventuell nemnd.

5.5 Skadelig og harmfullt innhold

I tillegg til dette vil en nemnd kunne ha en funksjon i forhold til det en betegner som skadelig og harmfullt materiale. Det typiske eksempelet er barnepornografi. Slikt materiale er både forbudt å produsere, besitte og videreformidle offentlig, jf. straffelovens §§ 204 og 204a. Det er også bred konsensus om at det bør være slik. Til bekjempelse av barnepornografi har Kripos i samarbeid med Telenor innført et såkalt filter som blokkerer slike sider. De facto foretas en effektiv blokkering av slike sider. Telenor og Kripos sensurerer etter deres oppfatning av hva som faller inn under bestemmelsene. Professor dr. juris Kare Lilleholt påpeker i den sammenheng følgende:[10]

> «Går ein først inn på den tankegangen som ligg bak ordninga, blir neste spørsmål om meir enn barnepornografi skal omfattast. Det finst andre ytringar som er ulovlege her i landet. Skal vi overlata til politiet å drive førehandssensur der og?
>
> Det å kunne gje og ta imot informasjon utan kontroll frå andre er eit stort gode. Eit slik gode kan misbrukast, som dei fleste andre gode, men det gjev ikkje utan vidare tilstrekkeleg grunn til å ta frå oss godet. Å føre kontroll med ytringar er makt, og makt må kontrollerast. Stort sett blir makt utøvd med forstand, men vi må alltid vera opne for at makta kan misbrukast. Det gjeld hos oss som andre stader og i dag som før: Makt må møtast med mistru.»

Undertegnede deler Lilleholts syn og er meget skeptisk til en stadig innskrenkning av ytringsfriheten. De steder der det likevel skjer, er det viktig at en har en ordning som sikrer en skikkelig behandling av grensetilfellene. Det er i det hele tatt betenkelig at ordningen med Telenor/Kripos' filter presses igjennom uten at en samtidig vurderer behovet for en judisiell kontroll. En nemnd som her diskuteres kan imidlertid tenkes å ha en funksjon også her. Det er ikke gjort noen systematisk undersøkelse i forhold til de sider som blokkeres, men det er grunn til å anta at blokkering av sider med lovlig innhold kan forekomme.

Et annet eksempel på skadelig materiale på Internett, vil være sider som oppfordrer til selvmord. Dette vil kunne være ulovlig, jf. straffelovens § 236.[11] Det kan i den sammenheng nevnes at flere land som for eksempel Australia og Frankriket har eksplisitte forbud mot nettsider som oppfordrer til selvmord.[12]

Nok et eksempel på skadelig innhold vil være spredning av datavirus. Det vil kunne rammes av straffelovens § 291 flg.[13]

5.6 Noen andre typer krenkelser som kan være relevante

Det finnes andre typer krenkelser som ikke helt lar seg passe inn i de tre nevnte typer. For det første har vi alle former for brudd på forbrukerrettigheter som kan finne sted på nettet. Slik jeg ser det, vil slike krenkelser fanges opp av andre ordninger, og det vil derfor ikke være naturlig for en nemnd som her foreslås å behandle disse. En klage på en nettbank vil for eksempel høre hjemme i Bankklagenemnda .

Andre typer tilfeller er de som faller inn under generalklausulen i markedsføringsloven av 16. juni 1972 nr. 47 § 1 om utilbørlig forretningsførsel næringsdrivende imellom. Slike tilfeller kan ligne både på krenkelser av immaterialrettslig art og kan være en form for integritetskrenkelse.

---

[10] Kaare Lilleholt: *Farleg fridom?* Lov og Rett 2006 s 1 - (LOR-2006-1).

[11] For en mer utførlig fremstilling se *Andreas Galtung og Ola-Kr. Hoff*. Selvmordsfare og Internett, kan jussen gi beskyttelse. Oslo 2007.

[12] Se *Andreas Galtung og Ola-Kr. Hoff*. Selvmordsfare og Internett, kan jussen gi beskyttelse. Side 105-112. Oslo 2007.

[13] Se for eksempel Inger Marie Sunde: *Lov og rett i Cyberspace*. Side 99. Oslo 2006.

En siste type krenkelser som også kan tenkes forekomme på Internett, er forbrytelser mot staten. En kan tenke seg at noen legger ut hemmelige dokumenter på nett. I så fall vil det melde seg et spørsmål om staten burde kunne klage. Jeg er selv av den mening at en nemnd som her foreslås, først og fremst bør være for publikum, men ikke begrenset til privatpersoner.

5.7 Konklusjon på virkeområde

Boks 2.1

Undertegnede er av den oppfatning at en nemnd bør ha et bredt virkeområde og i utgangspunktet kunne dekke de fleste typer av krenkelser på Internett. Om andre ordninger er relevante, kan nemnda ha som oppgave å sende saker som hører hjemme i andre organer videre.

6 Hvem vil en nemnd rette seg mot

6.1 Nettvertenes ansvar

Som utgangspunkt vil det være de som sørger for at krenkelsene eventuelt blir publisert som er ansvarlige. Det vil som regel være den som skriver noe krenkende eller tar et fotografi og laster det opp på nettet. I mellomstillingen kommer de som utelukkende har en teknisk formidler-rolle som nettvertene og televerksoperatørene som eier linjene. Det har vært mye fokus de senere år på hva slags ansvar en nettvert har. Det som er klart er at en nettvert kan komme i ansvar etter prinsippene i ehandelslovens § 18:[14]

> «*§ 18. Ansvarsfrihet for visse lagringstjenester*
>
> En tjenesteyter som lagrer informasjon på oppfordring fra en tjenestemottaker, kan bare
>
> a) straffes for lagring av ulovlig informasjon eller medvirkning til ulovlig virksomhet ved lagring av informasjon, dersom han har utvist forsett, eller
> b) holdes erstatningsansvarlig for lagring av ulovlig informasjon eller medvirkning til ulovlig virksomhet ved lagring av informasjon, dersom han har utvist forsett eller grov uaktsomhet.
>
> Tjenesteyteren er i alle tilfelle straffri eller fri fra erstatningsansvar dersom han uten ugrunnet opphold treffer nødvendige tiltak for å fjerne eller sperre tilgangen til informasjonen etter at forsettet eller den grove uaktsomheten etter første ledd forelå.
>
> En tjenesteyter er ikke ansvarsfri etter denne paragraf dersom tjenestemottakeren handler på tjenesteyterens vegne eller under hans kontroll.»

Dette er en komplisert bestemmelse. På den ene side statueres mye ansvarsfrihet. På den annen side forteller den oss i 3. ledd at vedkommende er fri for straff og erstatningsansvar *dersom det reageres uten ugrunnet opphold med å fjerne den ulovlige informasjonen*. Selv om det er snakk om en aktør som i utgangspunktet bare har en teknisk rolle, kan de altså komme i ansvar.

I utgangspunktet vil de kunne komme i ansvar fordi de bidrar til at ulovlig informasjon blir liggende, eller de kan komme i ansvar fordi de utestenger informasjon som er lovlig. Det kan skje fordi de ikke ønsker å ta risikoen med å komme i ansvar for å ha formidlet ulovlig informasjon. Avgjørelsen om hva som er lovlig eller ikke kan under tiden være vanskelig å ta og slett ikke alle nettverter har den erfaring, kunnskap og nødvendige ekspertise til å finne ut av det.

Dette gjør at en nemnd vil kunne virke meget befriende overfor en nettvert. Når en slik løsning eksisterer, vil de kunne henvise vanskelige tilfeller til nemnda og kunne si til den som er krenket og kunder at de følger avgjørelsen til en nemnd. På den måten kan de skyve et ansvar over på andre med de nødvendige kvalifikasjoner. Jeg er således ikke enig med dem som hevder at «nå må nettvertene ta ansvar». Hva som da menes er ofte uklart, og det er vanskelig å forstå hva slags ansvar en mener de skal ta. Om en ønsker å pålegge overvåkning og forhåndskontroll, vil det lett være i strid med prinsippene i ehandelsdirektivet slik det er formulert i ehandelslovens §§ 19 og 7:

> «*§ 19. Overvåking mv.*
>
> Bestemmelsene i §§ 16 til 18 medfører ikke at tjenesteyteren har en generell plikt til å kontrollere eller overvåke den informasjonen som lagres eller overføres på oppfordring fra en tjenestemottaker, eller en generell plikt til å undersøke forhold som antyder ulovlig virksomhet.
>
> *§ 7. Forbud mot krav om forhåndsgodkjenning*
>
> En tjenesteyter kan tilby informasjonssamfunnstjenester uten noen forhåndsgodkjenning eller lignende tillatelse, som utelukkende

[14] Jon Bing: *Ansvar for ytringer på nett*. Side 198 flg. Oslo 2008.

har sin grunn i tilbudet om informasjonssamfunnstjenester.

Krav om tillatelse til å bruke begrensede ressurser etter ekomloven, jf. kapitlene 6 og 7, gjelder uten hinder av første ledd.»

For å få en ordning til å fungere, er det klart at en trenger å kunne rette avgjørelsen mot nettverter av den enkle grunn at de er forholdsvis enkle å finne, og videre at det er de som har mulighet til å stoppe informasjonen dersom det trengs. Enkelt sagt: De kan trekke ut pluggen og det er de som må bli pålagt å gjøre det dersom utgiver/ originær ytrer ikke vil stoppe informasjonen selv. Det vil lett kunne være at de ikke vil, eller for den saks skyld er vanskelig å få tak i. Det riktige vil imidlertid være at man først henvender seg til den som er ansvarlig for informasjonen og starter med å prøve å få til en løsning,

Går ikke det vil det kunne bli spørsmål om å be nettverten stenge siden. Det er selvfølgelig siste utvei.

6.2 Fordeler særlig for næringen, særlig nettvertene

Når det gjelder fordelene for publikum, synes de åpenbare særlig når det gjelder krenkelser av personvernmessig art. De vil få et sted å henvende seg. De slipper å gå til advokat og ta den belastningen det kan være. Dagens situasjon er at svært mange slike saker som regel vil bli henlagt med mindre det er snakk om veldig alvorlige lovbrudd, og ikke bli ført dersom de er sivilrettslige. Det vil som regel være for kostbart.

For næringen og da særlig for nettverter, vil det være flere fordeler med en nemnd: De vil kunne spare betydelige summer og andre belastninger på å slippe selv å foreta vurderinger om materialet er lovlig eller ikke. Det var i sin tid viktig i argumentasjonen for ønsket om Nettnemnda. De vil kunne hevde sin nøytralitet overfor sine kunder og si at de forholder seg som andre ved spørsmål om stengning. I den sammenheng skal en være klar over at en nemndsavgjørelse også kan gå ut på at noe ikke er en krenkelse. Også det kan være en avgjørelse som en nettvert ikke vil ønske å være ansvarlig for.

Et annet særdeles viktig moment er at om en nettvert har fulgt et pålegg fra en kvalifisert nemnd kan det i seg selv være ansvarsbefriende. I forbindelse med implementering av ansvarsreglene i ehandelsloven ble det uttalt i forarbeidene følgende i forhold til straffeansvar:[15]

«Dersom nettverten foretar en aktsom vurdering av den aktuelle informasjonen, bør han kunne påberope seg ansvarsfrihet. Tilsvarende også om nettverten har henvendt seg til kompetente organer, som f.eks. Nettnemnda, dersom nettverten selv mangler den nødvendige juridiske kompetanse.»

I forhold til vurderingen av erstatningsansvar som krever grov uaktsomhet, jf. ehandelslovens § 18 for at erstatning kan ilegges, sies det at:[16]

«Hensynet til ytringsfriheten må tillegges betydelig vekt i vurderingen av hvilke forhold som anses som grovt uaktsomme. Avgjørende vil være om nettleverandøren har vurdert informasjonen seriøst, og ved dette funnet den lovlig. Har nettleverandøren valgt å henvende seg til aktører som har spesiell kompetanse, f.eks. Nettnemnda, kan nettleverandøren vanskelig anses for å ha handlet «grovt uaktsomt ».

Dette er åpenbart riktig juss og vil i seg selv være et meget sterkt insitament for nettverter og andre relevante aktører i lignende posisjon til å delta i en slik ordning. Rent konkret innebærer det da at dersom nemnda utferdiger et pålegg om utestengning av en kunde på grunn av en sides innhold, vil de dersom saken ender annerledes i rettsapparatet ikke kunne bli holdt ansvarlig. Likeså kan man tenke seg at nemnda uttaler at innholdet på en side ikke må stenges på grunn av injurier og at domstolene på et senere tidspunkt kommer til det motsatte, vil de heller ikke her kunne bli holdt ansvarlig. Det har ofte vært hevdet at nettverter heller vil stenge en side enn bli holdt ansvarlige og at det i seg selv kan ha en såkalt «chilling effect» i forhold til ytringsfriheten.

Om det skulle komme lovgivning på dette området, burde det kanskje eksplisitt bli sagt at de som følger pålegg fra en nemnd har fulgt kravene til aktsomhet og dermed ikke vil kunne ilegges medvirkningsansvar selv om en domstol ville komme til det på et senere tidspunkt.

En nemndsløsning vil videre føre til at praksis omkring nettkrenkelser vil bli mer likeartet i og med at alle i utgangspunktet vil forholde seg til samme organ.

---

[15] Innst.O.nr.46 (2003-2004). Innstilling frå næringskomiteen om lov om endringer i lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester (ehandelsloven) punkt 1.5 straffeansvar.

[16] Innst.O.nr.46 (2003-2004). Innstilling frå næringskomiteen om lov om endringer i lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester (ehandelsloven) punkt 1.5 erstatningsansvar.

Boks 2.2

Det er mange fordeler, hvorav nettverters utsikt til ansvarsfrihet vil gjøre at de selv vil ha interesse av at ordningen blir etablert. Om det skulle komme lovgivning på dette området burde det kanskje eksplisitt sies at de nettverter som følger pålegg fra en nemnd har fulgt kravene til aktsomhet og dermed ikke vil kunne ilegges medvirkningsansvar selv om en domstol ville komme til at forholdet ellers er ansvarsbetingende.

7 Hovedelementene i et tenkt regelverk

7.1 Litt om materielle regler for en tenkt nemnd

Formålet med et regelverk bør verken være å utvide eller innskrenke den ytringsfrihet og/eller det personvern som finnes i lovgivningen, men å gjøre håndhevingen av disse rettigheter mer effektiv og til en realitet.

I Nettnemndas regelverk var kanskje den viktigste bestemmelsen å finne i regelverkets punkt 4.3:

> «4.3 Utgiveren plikter å føre tilsyn med hva som gjøres tilgjengelig på eget nettsted og ta tilbørlig hensyn til allmennhetens interesser og andres rettigheter så som æresvern, personvern, immaterielle rettigheter mv.»

Kombinert med at forholdet i alle saker måtte avbalanseres i forhold til bestemmelsene i EMK artikkel 8 og 10, har en her en rekke bestemmelser som egentlig ikke sier mer enn at det dersom det er snakk om rettigheter beskyttet i lov av typen som nevnt ovenfor, vil det kunne reageres. Bestemmelsen her er som en ser ikke presis når det gjelder kategorien skadelig harmfullt materiale. Det vil en måtte ta stilling til i et eventuelt nytt regelverk.

I tillegg til dette vil en måtte ta stilling til om en ønsker spesielle regler som for eksempel tilsvarsrett. Nettnemndas regelverk hadde en bestemmelse om dette, men den ble aldri praktisert.

Nok et spørsmål er hvorvidt et regelverk også skal ha regler om kommunikasjon: Nettnemndas regelverk hadde en regel om det i punkt 4.5:

> «4.5 Kommunikasjon på Internett skal ta tilbørlig hensyn til god nettskikk, og vesentlige brudd på denne plikt kan bringes inn for Nemnda.»

En slik bestemmelse kunne tenkes å ramme uønsket e-postreklame (spam), men der har man nå egne regler i markedsføringslovens § 2b. Den kunne videre tenkes å ramme sjikanøs opptreden i e-post eller lignende.

7.2 Prosessuelle regelverk

Hovedelementene er selvsagt at man bør ha kontradiksjon. Blir noen klaget inn for noe, bør en få komme med et tilsvar og selvsagt også gis sjanse til å rette opp forholdet.

Et særskilt spørsmål er om hvem som skal gis klagerett. Bør det være snakk om rettslig interesse, slik det er krav om i sivilprosessen eller bør det være mindre strenge krav? For Nettnemndas del hadde man i regelverket en regel om at Nettnemnda kunne ta opp saker av eget tiltak, lik det det nå nedlagte Teletorgrådet også hadde. Denne regelen var i sin tid hentet fra det tilsvarende klageorganet i England ICSTIS nå Phonepay Pluss.[17] En slik bestemmelse kan imidlertid fort få nemnda til å se ut som et slags nettpoliti. Selv om det vil være ønskelig med en mulighet til å se på saker etter eget initiativ, er nok det en regel som vil møte stor motstand. Det som uansett er viktig er at dersom en nemnd skal kunne fungere, må kravene til klageinteresse ikke være for snever. Pressens faglige utvalg har i sine vedtekter følgende regel i § 5, 5. ledd:

> «I utgangspunktet kan alle klage. Dersom klager ikke er identisk med den eller dem saken gjelder, skal det som hovedregel innhentes samtykke fra disse. Når særlige forhold tilsier det, kan PFU bestemme at klagen behandles uten at samtykke er innhentet. I slike saker skal PFU samtidig drøfte om det skal gjøres unntak også fra hovedregelen om offentlighet i § 6.»

Her er altså hovedregelen at det skal foreligge en klage fra en med tilknytning til saken, men at det kan gjøres unntak. Dette er en regel en bør vurdere. Om en ikke kan avgjøre saker ved eget tiltak, bør nemnda kunne uttale seg av eget tiltak.

Et spørsmål er om man for eksempel skal kunne godta anonyme klager. Et argument for det, er at det kan tenkes, at mange typer klager ikke vil komme dersom klager må identifisere seg. En

[17] http://www.phonepayplus.org.uk/

kan tenke seg at noen ønsker å klage på at Kripos' barnepornografifilter stenger adgang til et nettsted fordi det oppfattes som ulovlig barnepornografi. Dersom nettstedet i seg selv er tvilsomt er det ikke sikkert at noen vil klage dersom det innebærer identifikasjon.

Boks 2.3

En tenkt nemnd bør ha kontradiksjon, det bør ikke være for snevre krav til klageinteresse og det bør vurderes om en skal kunne godta anonyme klager. Uansett bør en nemnd kunne avgi veiledende uttalelser av eget tiltak.

7.3 Organisering

Når det gjelder organisering henviser jeg til det som sies nedenfor under punkt 10.

7.4 Forholdet til andre nemnder og klageordninger

I et regelverk som etablerer en ny nemnd (og ikke legger funksjonene til et eksisterende organ) bør regelverket si noe om forholdet til andre organer. Det er flere andre nemnder/tvisteløsningsorganer som kan tenkes å behandle forhold relatert til Internett. Dersom dette er mer spesialiserte nemnder bør en nemnd ha som oppgave å videresende relevante saker dit. I så måte kan en seg at nemnda inngår et samarbeid med nemnder der denne problemstilling kan tenkes å oppstå. Som eksempel på dette kan nevnes saker som faller inn under Pressens faglige utvalg (PFU). PFU har siden de første gang tok stilling til egen kompetanse i forhold til nettmedia i 1996 behandlet flere saker relatert til Internettpublisering.[18]

PFU er en vel etablert ordning som synes å fungere, og det vil av den grunn ikke være naturlig at slike saker også behandles av her foreslåtte nemnd. Det samme vil gjelde saker om tjenestekjøp på nett som behandles av ulike forbrukerklagenemnder. En klage om forhold på en forbrukers nettbank hører selvfølgelig hjemme under Bankklagenemnda.

[18] Uttalelse fra PFU 17.6 1996.

7.5 Særlig om forholdet til Datatilsynet/ Personvernnemnda

Et spørsmål er hvordan en håndterer forholdet til Datatilsynet/Personvernnemnda. Personvernnemnda behandler først og fremst klager på Datatilsynets vedtak etter personopplysningsloven. Opprinnelig hadde Datatilsynet lagt til grunn at hjemmesider med personlige og private formål lå utenfor anvendelsesområdet for personopplysningsloven. Dette ble imidlertid endret etter praksis fra EF-domstolen i form av prejudisiell avgjørelse i 2003.[19] Et stort antall nettsteder vil som følge av denne praksis være omfattet av personopplysningsloven, mens andre vil falle utenfor, jf. personopplysningslovens § 7 som eksplisitt unntar sider som er av *kunstneriske, litterære eller journalistiske, herunder opinionsdannende, formål.*[20] Denne grensen har vært drøftet i flere vedtak av Personvernnemnda. I en klagesak fra 2005 gjaldt saken nettsteder som inneholdt navn på over 400 personer som hadde hatt befatning med barnevernsaker. Flere av de omtalte klaget til Datatilsynet, men Personvernnemnda anså til slutt at nettsiden falt utenfor personopplysningsloven da den kom inn under unntakene i § 7.[21] Et annet eksempel finnes i klagesak 2005-14. Saken gjaldt Datatilsynets pålegg om å slette personopplysninger på hjemmesiden til karatestilartsorganisasjonen Shorin Ryu Karate Association Norway. Personvernnemnda kom til at klubbens hjemmeside ikke var omfattet av personopplysningslovens § 7 og denne bestemmelsens begrep «journalistisk formål»; og dermed vernet av ytringsfriheten.[22] Veldig mange nettsteder/hjemmesider er det. Når det gjelder andre typer hjemmesider ser en at Datatilsynet har kommet med en del uttalelser selv om personopplysninger på Internett. I et innlegg på egen hjemmeside sier Datatilsynet om deres rolle, dersom en finner uønskede opplysninger om en selv på internett, følgende:

> «Datatilsynet kan hjelpe deg med personvernrelaterte saker. Antallet slike saker vil avgjøre om disse vil bli behandlet samlet mot den som publiserer innholdet, eller om Datatilsynet vil ta dem som enkeltsaker. På grunn av at lovgivningen er forholdsvis ny på feltet, samt at muli-

[19] Se Case C-101/01.

[20] Se også Jon Bing: *Ansvar for ytringer på nett*. Side 176-181.

[21] KLAGESAK 2005-03: Klage på Datatilsynets vedtak om avvisning. Personvernnemndas avgjørelse av 9.6.2005. se http://www.personvernnemnda.no/vedtak/2005_3.htm

[22] Se for eksempel. Personvernnemnda klagesak 2005-14. Avgjørelse av 26. mai 2006. og

ge personvernrelaterte saker vedrørende publisering på Internett kan bli omfattende, vil vi være forsiktig med å love kort saksbehandlingstid for denne typen saker.[23]»

Det er grunn til å anta at Datatilsynet vil ønske velkommen en ordning som kan arbeide raskt. Selv om det kan være kompetanseoverlapp i form av at krenkelser kan dekkes av begge organer.

Spørsmålet er så hvordan en løser det. En løsning er å si at saker som hører inn under Datatilsynet ikke skal behandles av nemnden. En annen løsning ville være å si det omvendte ut i fra en lex posterior (at nyere lover går foran eldre) tankegang. Begge disse løsninger har lite for seg.

Et annet poeng er at dersom nemndas oppgave og sanksjoner først og fremst skal gå ut på å stanse materialet som nemnden anser at kan være ulovlig. En slik handling behøver ikke være problematisk i forhold til Datatilsynets kompetanse. Det er ikke grunn til å tro at Datatilsynet vil være i mot at en annen nemnd har mulighet til å stenge sider som den anser har ulovlig innhold.

Så kan en tenke seg de tilfeller at nemnden kommer til at en hjemmeside ikke har ulovlig innhold, mens Datatilsynet på sin side mener den strider mot personopplysningsloven. Selv dette bør i utgangspunktet ikke være mer spesielt enn tilfeller der et overordnet organ kommer til en annet enn underordnet organ. En pragmatisk løsning å velge for de tilfellene er at Datatilsynet selv velger sin tolkning av det regelverket de er satt til å forvalte. Om de velger å legge vekt på et tidligere vedtak fra nemnden eller ikke er opp til dem.

Så kan en tenke seg det omvendte tilfelle, nemlig at nemnden stenger en side, mens Datatilsynet i en senere vurdering kommer til at innholdet er uproblematisk. Spørsmålet da blir hvordan nemnden skal forholde seg til det. Det er tre løsninger:

1. hva Datatilsynet mener og vedtar påvirker ikke nemndens vedtak. Nemndens vedtak skal bare kunne overprøves av domstolene.
2. en kan tenke seg at nemnden i slike tilfeller er forpliktet til å heve stengningen, og at dette nevnes eksplisitt i et tenkt regelverk.
3. nemnden er bare forpliktet til å heve vedtaket om stengning dersom det er klart nemnden i det vesentligste har bygget på henvisninger til lovgivning som Datatilsynet har ansvaret for.

Selv mener jeg den beste løsningen er at organene får kompetanse uavhengig av hverandre, men at de samtidig inngår et nært samarbeid. En skal ellers merke seg at Personopplysningsloven har ganske omfattende sanksjoner, §§ 46-49 som inneholder bestemmelser om: Pålegg om endring eller opphør av ulovlige behandlinger (46), tvangsmulkt (47), Straff (48), Erstatning (49). En kan her særlig merke seg at Datatilsynet har adgang til å ilegge tvangsmulkt dersom pålegg ikke følges. Dette sanksjonsapparatet bør heller ikke ha noe å si for virksomheten til en tenkt nemnd. Om en nemnd skulle komme til at innhold på et nettsted side må fjernes eller pålegge stengning, vil sanksjonene etter personopplysningloven kunne vurderes helt uavhengig av det.

Når det ellers gjelder kompetanseoverlapp er ikke det noe uvanlig. Dette har for eksempel i ganske stor grad vært tilfelle for så vidt angår Post- og teletilsynet og Konkurransetilsynet, i og med at både konkurranselovgivning og telelovgivning til dels har hatt overlappende regler. Mellom disse etatene er det inngått en egen avtale som tar sikte på å løse eventuelle problemer i den forbindelse.[24]

8 Sanksjoner og hjemmelsgrunnlag

8.1 Innledende bemerkninger

Om en går inn for en nemnd blir et av de viktigste spørsmålene å avklare hva slags rettslig grunnlag nemnda skal ha. Skal den ha sanksjoner må den ha basis i lov eller avtale. Selvregulering er mye i vinden ut fra den tanke at aktuelle bransjer først og fremst bør ordne opp selv. E- handelsdirektivet oppfordrer til dette i artikkel 16 og 17 der det sies:

«Article 16
Codes of conduct
1. Member States and the Commission shall encourage:
(a) the drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of Articles 5 to 15;»

Og artikkel 17.1

[23] Datatilsynet, redaksjonen: *Uønsket informasjon om deg på nett?* (29.05.2008) Redaksjonen, datatilsynet.no

[24] Avtale om samarbeid, samordning og oppgavefordeling mellom Konkurransetilsynet og Post- og teletilsynet. 28. februar 2005. se http://www.npt.no/iKnowBase/Content/50232/avtale_kt_pt.pdf

«Article 17

Out-of-court dispute settlement

1. Member States shall ensure that, in the event of disagreement between an information society service provider and the recipient of the service, their legislation does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means.»

Nå innebærer ikke dette direktivet en motstand mot eventuelle statlige spesialnemnder. Det er vel mer riktig å se på direktivet som en oppfordring til å få løst konflikter av den type som her kan oppstå utenfor det ordinære rettsapparatet. Konfliktløsning utenfor det ordinære rettsapparatet er ellers som nevnt helt i tråd med prinsippene for og en av grunnene til reformen med den nye tvisteloven av 2005.[25] I forarbeidene sies det eksplisitt at *Det er et mål både at tvister om mulig kan bli løst utenfor domstolene, og lette tilgangen til domstolene i saker der det er behov for det.* [26]

Når det gjelder etablering av en nemnd slik jeg ser det er det tre alternativer:

Selvreguleringsnemnd som må baseres i avtale.

Offentligrettslig basert nemnd.

En kombinasjon av de to, gjerne omtalt som c-regulering.

Selvreguleringsordninger er absolutt i vinden. Mye av forbrukersektoren har ordninger basert på selvregulering, eller som har begynt som selvregulering og senere fått en offentligrettslig basis. Både Bankklagenemnda og Forsikringsklagenemnda har en forankring i lovgivningen selv om de er basert på avtale.

Det som finnes av forbrukernemnder kan gjerne omtales som bransjenemnder hvilket vil si at de behandler klager innenfor en bransje, Når det gjelder det som utredes her, nemlig en klagenemnd for Internettkrenkelser, er det ikke snakk om en bransjenemnd. Internett er jo ingen bransje selv om man snakker om bransje for dem som for eksempel tilbyr lagring og adgang til nettet for øvrig. Internett inneholder egentlig alt.

Da Nettnemnda i sin tid ble etablert var det hovedsakelig to hovedgrunner til det. For det første ønsket nettvertene å spare interne utgifter til juridisk rådgivning, og for det andre var en usikker på hva lovgivningen ville komme frem til om nettvertansvar. Da arbeidet begynte ventet man på ehandelsdirektivet. Bransjen, særlig i form av nettvertene så det som formålstjenlig å vise at man selv tok ansvar og etablerte derfor den avtalefestede nemnda Nettnemnda.

8.2 Sanksjoner

Hva slags løsning en går for med hensyn til grunnlaget, vil ha sammenheng med hva slags sanksjoner en ønsker at nemnda skal ha. På forbrukersektoren er det slik at mange nemnder utelukkende gir veiledende avgjørelser. Dette fungerer bra der man har seriøse bransjer som alltid på sikt vil gjøre best i å følge avgjørelsen til den aktuelle nemnda. Både Bankklagenemnda og Forsikringsklagenemnda er eksempler på dette selv om det også finnes eksempler på at nemndavgjørelser ikke er blitt fulgt. På et område hvor en har alt mulig og ingen enhetlig bransje, kan det slås fast med en gang at en nemnd som bare kan gi veiledende avgjørelser ikke vil fungere.

Neste spørsmål blir hva slags sanksjoner en ønsker at en nemnd skal ha. Spørsmålet blir i hvilken grad en ønsker at nemnda skal kunne:

Straffe, ilegge erstatning, foreta inndragning eller bare kunne sørge for å stoppe et internettkrenkelse som anses som ulovlig og herunder kunne pålegge retting.

Jeg vil i denne rapporten ikke gå mye inn på dette, men fastslå at en nemnd som dette ikke bør kunne ha noen sanksjon utover det å stoppe en nettkrenkelse som er ulovlig. Andre sanksjoner som straff eller erstatning bør avgjøres av domstolene og eventuelt andre organer som måtte ha den muligheten, slik det ellers er vanlig. Selv stengning eller blokkering av informasjon på nettet er en meget inngripende sanksjon og bør bare forekomme som siste utvei etter at man har pålagt retting. En annen sak er at dersom en nemnd skulle drive med erstatningsutmåling og eventuelt straffe som oppgave ville det kreve ytterligere ressurser. Det forberedende lovarbeide ville nødvendigvis også bli mer komplisert. På den annens side kunne en tenke seg at nemnda fikk anledning til anbefale erstatning eller å påpeke i vedtak at en handling er erstatningsbetingende.

Boks 2.4

Når det gjelder sanksjoner bør det først og fremst være snakk om pålegg om retting, sletting og/eller stengning slik at krenkelsene opphører.

[25] Lov om mekling og rettergang i sivile tvister (tvisteloven). LOV-2005-06-17-90

[26] Se Ot.prp. nr. 51 (2004-2005) om lov om melding og rettergang i sivile tvister (tvisteloven), s. 13.

8.3 Avtale som hjemmel – selvregulering

For at en avtalefestet nemnd skal virke, er det nødvendig at de som kan komme ulovlige Internettkrenkelser til livs deltar. Dette er først og fremst nettverter og ellers teleoperatør som er med ogbesørger transporten. Teleoperatører kan til en viss grad blokkere tilgang til Internett. Et eksempel på det er filtreringen som foretas i forbindelse med barnepornografi.

En slik nemnd må da baseres i et regelverk som så partene avtaler seg imellom at de vil følge. Ordningen må for å fungere ha følgende komponenter:

Materielle regler

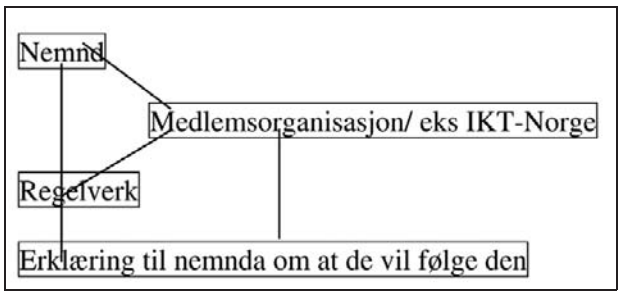
Prosessuelle og organisatoriske regler

Erklæring eller avtale om at nettverter følger pålegg fra nemnda

Avtale mellom nettverter/ teleoperatører og deres abonnenter:

Dette gir modell som i figur 2.2.

I praksis var dette modellen for Nettnemnda. Svakheten med en selvreguleringsmodell som dette er at det er vanskelig å få alle med. Det kan videre være snakk om veldig forskjelligartede aktører. Mange vil være skeptiske til å overlate avgjørelsesmyndighet til andre. Videre vil mange mene at de spørsmål ordningen ønsker å løse ikke er noe problem og at det uansett ikke angår dem. Det som imidlertid er mest problematisk er at en avtalebasert selvreguleringsordning vil koste penger som vil måtte dekkes av bransjen selv. Det var som nevnt finansieringen som viste seg å være problematisk i forhold til Nettnemnda. En annen utfordring vil være å finne en rettferdig finansieringsmodell. En kan teoretisk tenke seg mange modeller og kombinasjoner. Felles for dem alle vil nok være at mange deltagere lett vil føle at de rammes av dem på en urettferdig måte.



Figur 2.2

Omsetning

En kan tenke seg finansiering på grunnlag av nettvertenes totale omsetning.

Dette vil fungere dårlig for dem som bare i liten grad driver med relevante tjenester. En kan selvfølgelig tenke seg at en tok utgangspunkt i hva medlemsbedrifter i IKT-Norge betaler i medlemsavgift og beregne ut fra det. Medlemsavgiften beregnes ut fra bedriftens omsetning. Dette er også vanskelig da det kan være uklart å finne hvor mye som skriver seg fra den Internettrelevante omsetning.

Abonnenter

En kunne tenke seg en avgift på antall abonnenter nettverten har, en flat avgift eller del av det de selv tar fra abonnenten. Alternativt ta det inn på antall domener de er nettvert for. Også det er vanskelig: prisene er veldig forskjellige, og hvordan skulle en gjøre det i forhold til dem som ønsker å tilby gratis nettvertskap (hosting).

Avgift for enkelt klager

En kan tenke seg at det ilegges gebyrer for dem som mottar klager mot seg. Det vil imidlertid være prinsipielt urimelig i forhold til nettverter som i utgangspunktet ikke er annet enn nettverter som tilbyr lagringsplass. Nettvertene vil imidlertid kunne ta det inn i abonnementskontrakten at utgifter med eventuelle klager på dem som er innklaget kan inndrives dersom de viser seg å være riktige. Spørsmålet blir da om nemnda kommer til at det dreier seg om en innholdsløs klage. Hvem skal da bære utgiftene? Innklagede, slik tilfellet er når man taper en sak? Er det snakk om et meget beskjedent gebyr vil det kanskje ikke spille noen rolle. Er det derimot snakk om å velte risiko over på klager vil ordningen lett bli meningsløs.

Konklusjon på finansieringsmodeller

På bakgrunn av det som er nevnt ovenfor er det min mening at det å finne en finansieringsmodell som bransjen vil akseptere vil være meget vanskelig. Jeg tror at dette vil være en av de største hindringene for å kunne etablere en nemnd som skal kunne fungere. Og en nemnd vil nødvendigvis koste penger om den skal kunne fungere effektivt.

Jeg tror det vil være vanskelig å få finansiert denne nemnda privat, samt å finne en alternativ modell som vil kunne fungere rettferdig. Av den

grunn vil en løsning med en avtalefestet bransjenemnd ikke fungere. En kan imidlertid tenke seg at en avtalefestet nemnd vil fungere dersom det bevilges til den fra det offentlige.

8.4 En offentlig-rettslig basert nemnd

I og med at det vil være vanskelig få på plass en økonomisk selvbærende, avtalefestet nemnd, er spørsmålet om ikke dette bør være et statlig ansvar, og at det offentlige bør etablere en nemnd med et tilstrekkelig mandat. I og med at internettkrenkelser ikke nødvendigvis kan henføres til en bransje, vil det kunne være et argument at dette nettopp er noe som det offentlige bør ta ansvar for. På den annen side synes mange og da særlig fra pressehold, å være særdeles kritisk til en slik ordning.

Mange vil nok hevde at i og med at deler av Internettbransjen har ansvar for innhold bør de selv ha interesse for og finansiere en selvregulerende ordning. Mot dette kan anføres at nettopp det at det dreier seg om viktige spørsmål som ytringsfrihet og personvern gjør at en slik ordning bør ha en offentligrettslig basis. Det vil jo tross alt være mer demokratisk om dette er noe lovgiver har ansvaret for enn at det er noe som bestemmes av en bransje alene.

Dette har noe for seg om følgende kan oppfylles:

En nemnd må ha som formål å forhindre krenkelser på Internett, og da kanskje mest forhindre krenkelser av personvernmessig- og dernest opphavsrettslig karakter, samt skadelig og harmfullt materiale. For å få det til må det overbevises om at hensynet til ytringsfriheten vil bli vel ivaretatt.

Jeg tror i den sammenhengen at det vil være nyttig å gjøre slik man hadde det i Nettnemndas regelverk, nemlig påpeke at det ligger i formålet med regelverket å ivareta hensynene til ytringsfriheten slik denne er nedfelt i EMK artikkel 10 og i hensynet til personvernet i EMK artikkel 8.

Videre vil det jo ikke være slik at den tenkte nemnda kommer istedenfor domstolene.

Nemnda må fremstå som et nødvendig tilbud til publikum.

For at det skal være noen mening i å opprette en slik nemnd må behandling i nemnda være gratis, eller så godt som gratis.

8.5 Co-regulering /organisering

Så er spørsmålet om en kunne tenke seg en co-reguleringsordning. Det finnes en del eksempler på klageordninger som både har basis i avtale og lov. Som eksempel kan jeg her nevne Forsikringsklagenemndene. Disse er basert i avtale, men er også nevnt i Forsikrings-avtaleloven av 16. juni 1989 nr. 69 § 20-1:

> «§ 20-1. (nemndbehandling av tvister)
> Dersom det på grunnlag av avtale mellom selskapenes organisasjoner og forsikringstakernes organisasjoner eller Forbrukerrådet er etablert en nemnd for behandling av tvister i forsikring, og vedtektene er godkjent av Kongen, kan hver av partene kreve nemndbehandling av en tvist hvor nemnda er kompetent. Så lenge en tvist er til behandling i nemnda, kan ikke selskapet bringe den inn for de alminnelige domstoler. En sak som nemnda har realitetsbehandlet, kan bringes direkte inn for tingrett.»

Grunnlaget for nemndene er en avtale mellom Forbrukerrådet, Finansnæringens Hovedorganisasjon og Næringslivets Hovedorganisasjon (NHO). Avtalen som i dag regulerer Forsikringsklagekontoret og nemndene, ble senest revidert 18.11.1997.

Et annet eksempel er Bankklagenemnda. Denne er basert på lignende type avtale samtidig som den har en basis i Finansavtaleloven av 25. juni 1999 nr. 46:

> «§ 4. Nemndsbehandling
> (1) Gjennom avtale mellom en finansinstitusjon eller en lignende institusjon eller en organisasjon for slike institusjoner på den ene siden, og på den annen side Forbrukerrådet eller en annen organisasjon som representerer institusjonenes kunder, kan det opprettes en eller flere nemnder for behandling av tvister om finansavtaler.
> (2) Partene kan forelegge avtalen for Kongen til godkjenning. Har Kongen godkjent nemndas vedtekter, gjelder bestemmelsene i tredje til femte ledd.
> (3) Kunden kan kreve nemndsbehandling av enhver tvist hvor nemnda er kompetent, såfremt kunden har saklig interesse i å få nemndas uttalelse i saken. Tvist om urettmessig belastning av konto eller urettmessig bruk av betalingsinstrument, jf. § 37, kan også institusjonen bringe inn for nemnda.
> (4) Så lenge en tvist er til behandling i nemnda, kan ikke en part bringe den inn for de alminnelige domstoler. Bestemmelsen i første punktum er likevel
> ikke til hinder for tvangsfullbyrdelse etter tvangsfullbyrdelsesloven eller midlertidig sikring etter tvisteloven.
> (5) En sak som nemnda har realitetsbehandlet, kan bringes direkte inn for tingrett.»

En kunne godt tenke seg at definerte aktører fikk mulighet til å forhandle frem en reguleringsordning med en nemnd og at denne fikk en offentligrettslig «velsignelse» som dette.

8.6 Konklusjon med hensyn til rettslig grunnlag

Jeg har tidligere redegjort for vanskelighetene med å få deltagere i forsøket med Nettnemnda. Jeg tror imidlertid det hovedsakelig dreier seg mer om motvilje mot en ordning som medfører utgifter enn motvilje mot ordningen i seg selv. Uansett om en velger selvregulering, co-regulering eller en offentligrettslig basert nemnd, vil det argumenteres med betydelige fordeler for den del av næringen hvor det er relevant.

Boks 2.5

Det anbefales at en får på plass en nemnd med et offentligrettslig grunnlag.

9 Hjemmelsgrunnlag for nemnda

Dersom nemnda skal ha sanksjoner og treffe bindende avgjørelser vil den måtte ha et hjemmelsgrunnlag. Et spørsmål i så måte er om det finnes relevant lovgivning som eventuelt vil kunne hjemle opprettelsen av en nemnd av den typen en tenker seg:

En nærliggende lov å lete i er ehandelsloven. Denne loven har en rekke forskriftshjemler hvor av en kan merke seg den i § 17:

> «§ 17. Ansvarsfrihet for visse mellomlagringstjenester
>
> En tjenesteyter som nevnt i § 16 første ledd, er ikke strafferettslig eller erstatningsrettslig ansvarlig for innholdet i informasjon som automatisk, mellomliggende og midlertidig lagres utelukkende for å gjøre overføringen til andre tjenestemottakere mer effektiv, forutsatt at tjenesteyteren
>
> a) ikke selv bestemmer eller endrer informasjonen som overføres,
> b) overholder vilkår for tilgang til informasjonen,
> c) overholder alminnelig godtatte regler for oppdatering av informasjonen og
> d) ikke griper inn i lovlig anvendelse av alminnelig anerkjent teknologi, i den hensikt å oppnå data om bruken av informasjonen.
>
> Ansvarsfrihet etter første ledd gjelder bare dersom tjenesteyteren uten ugrunnet opphold fjerner eller sperrer tilgang til den lagrede informasjonen når tjenesteyter har fått kunnskap om at en domstol, en offentlig myndighet eller et særskilt organ utpekt av departementet i forskrift har gitt pålegg om å fjerne eller sperre tilgangen til informasjonen. Det samme gjelder når tjenesteyter har mottatt underretning om at informasjonen er fjernet fra opprinnelsesstedet eller at tilgangen til informasjonen er sperret.»

I siste ledd står det blant annet at ansvarsfrihet kan komme på tale dersom det ulovlige materiale fjernes eller tilgang sperres uten ugrunnet opphold. Det fremheves videre som en ser at et slikt pålegg kan komme fra domstol, offentlig myndighet eller et *særskilt organ utpekt av departementet i forskrift har gitt pålegg om å fjerne eller sperre tilgangen til informasjonen.* Selv om denne bestemmelsen er noe upresis er det utvilsomt ment som en forskrifts hjemmel for å kunne etablere et organ av den typen som diskuteres i denne rapporten. I forarbeidene hetter det at

> «Departementet ser at det kan være aktuelt å åpne for at også andre enn domstolenes eller offentlig myndigheters avgjørelser skal kunne føre til at tjenesteyteren må fjerne ulovlig materiale. På bakgrunn av dette innføres det en hjemmel for departementet til å i forskrift utpeke et organ som kan treffe avgjørelser som fører til at tjenesteyteren må fjerne det aktuelle materialet.»

Om en tar det som her sies i betraktning synes det åpenbart at en her har en tilstrekkelig forskriftshjemmel.

Om en skulle velge å se bort fra ehandelsloven vil lov om elektronisk kommunikasjon være en mulighet. Der kan det også slås fast at det ikke er noen forskriftshjemmel som kunne gi grunnlag for opprettelse av en klagenemnd for behandling av Internettkrenkelser. Dette er i stor grad også en fullmaktslov. Det kan imidlertid med sikkerhet slås fast at det ikke finnes noen hjemmel i denne loven som er vid nok til å hjemle en klagenemnd som her foreslås.

En kan imidlertid merke seg ekomloven av 4. juli 2003 nr.83 § 2-12. I denne fullmaktsbestemmelsen hjemles klageordninger for fellesfakturerte tjenester. Fellesfakturerte tjenester eller teletorgtjenester, som det gjerne ble kalt tidligere, er nå definert i ekomlovens § 1-5:

«15. fellesfakturert tjeneste: forhåndsbetalt og etterskuddsbetalt innholdstjeneste som tilbys over elektronisk kommunikasjonsnett og som faktureres sammen med elektronisk kommunikasjonstjeneste.»

§ 2-12 hjemler de klageordninger som i dag finnes i ekomforskriften av 16. februar 2004 nr401 og som inntil 1. juli 2008 fantes i teletorgforskriften av 1994. Denne forskriften hadde mange bestemmelser som regulerte innholdet og ga hjemmel til å opprette en avtalefestet nemnd som i sin tid behandlet innholdsklager. Et litt interessant poeng var at man helt fra 1994 da man fikk teletorgforskriften hjemlet denne i den gamle telegrafloven av 1899. Det spesielle var at dette var en fullmaktslov som egentlig ikke sa noen ting annet enn at man bare kunne drive telekommunikasjon dersom man hadde tillatelse fra Kongen. Da man i 1995 fikk en lov om telekommunikasjon anslo man forholdet hjemlet der, men det var først senere at man fikk inn en presis hjemmel for å regulere fellesfakturerte tjenester (teletorgtjenester). Dette kan jo ha vært en anerkjennelse av at man i flere år ikke hadde hjemmel for den innholdsreguleringen man opererte med på teletorg. Det finnes altså en hjemmel for å regulere innholdstjenester, men denne er begrenset til de fellesfakturerte, altså de tilfeller der det foreligger en betaling for innholdet samtidig med bruken.

Selv om dette er en bestemmelse som er ment å gi adgang til en viss form for innholdsregulering, er det klart at den ikke vil kunne tjene som grunnlag for å regulere en mer alminnelig nettklagenemnd.

9.1 Hvilken lov burde kunne hjemle en nemnd

Ehandelsloven synes som nevnt å ha den tilstrekkelige hjemmel. Det kan også bemerkes at også Ehandelsdirektivet, som er grunnlaget for loven, som nevnt oppfordrer til selvregulerende nemnder (out of court settlement).

En mulig hjemmelslov er også ekomloven. Jeg har allerede redegjort for hjemlingen av fellesfakturerte tjenester. Lovens formål fremgår av § 1-1 som lyder:

«§ 1-1. Formål

Lovens formål er å sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester, gjennom effektiv bruk av samfunnets ressurser ved å legge til rette for bærekraftig konkurranse, samt stimulere til næringsutvikling og innovasjon.»

Mens saklig virkeområde omtales i § 1-2 som lyder:

«§ 1-2. Saklig virkeområde

Loven gjelder virksomhet knyttet til overføring av elektronisk kommunikasjon med tilhørende infrastruktur, tjenester, utstyr og installasjoner. Forvaltning og bruk av det elektromagnetiske frekvensspekteret og nummer, navn og adresser er omfattet. Det samme gjelder all utstråling av elektromagnetiske bølger fra elektronisk kommunikasjon og all utilsiktet utstråling av elektromagnetiske bølger som kan forstyrre elektronisk kommunikasjon.

Kongen kan ved enkeltvedtak eller forskrift avgjøre hva som skal anses å falle innenfor lovens saklige virkeområde.»

Slik jeg ser det vil en nemnd kunne passe inn under denne loven. Det gjelder spesielt om en går for en nemnd med brett nedslagsfelt. I så måte er det en fordel at dette verken er en handels-, personvern- eller en immaterialrettslov.

Lovteknisk ville en kanskje kunne ta det inn i § 2-12 sammen med reguleringen av felles-fakturerte tjenester.

Ehandelsloven har kanskje en mangel ved at den synes å være en lov som begrenser seg til handel. Det behøver imidlertid ikke ha noe å si for den nemnden som her søkes etablert.

Boks 2.6

Ehandelsloven synes å kunne hjemle en Internettklagenemnd slik loven er i dag. Lov om elektronisk kommunikasjon (ekomloven) kunne også være hjemmel, men det forutsetter lovendring.

10 Organisering

10.1 Mandatutvidelse eller administrativ plassering

Dersom en går for en offentligrettslig nemnd vil spørsmålet om organisering reise seg. Det første spørsmålet er om det finnes etablerte ordninger som kunne få utvidet sitt mandat til å behandle nettkrenkelser av den type det redegjøres for i denne rapporten. Om det ikke er det, kan en stille

spørsmål om det finnes et organ som passer som administrativ myndighet.

10.2 Mandatutvidelse

Det første en kan stille spørsmål om er om det er noen nemnder, organer som er så nær behandling av de problemstillinger som her diskuteres at en kunne legge en ordning dit.

Personvernnemnda peker seg ut. Dette er imidlertid et klageorgan for avgjørelser fattet av Datatilsynet hovedsakelig når det gjelder vedtak med hjemmel i personopplysningsloven.

Medietilsynet kunne også tenkes, men heller ikke det er organisert på en slik måte at det enkelt vil kunne saksbehandle enkeltstående internettkrenkelser.

Av de forbrukernemnder som finnes, kunne en selvfølgelig tenke seg plassering hos en av dem, men disse har alle som mandat å håndtere forbrukerklager innenfor ulike sektorer. De vil sikkert blant mange bli oppfattet som å være for forbrukerorientert og derved ikke ha den tilstrekkelige nøytralitet som kan være ønskelig.

Fra pressehold har det vært foreslått at en ordning kunne etableres ved at man utvidet mandatet til PFU. Dette er en interessant tanke fordi PFU har erfaring med behandling av innhold. På den annen side er det stor forskjell på det å drive med presseetikk og spørsmål om immaterielle krenkelser og å ta stilling til ulovlig skadelig harmfullt materiale. Det er videre slik at PFU er et organ for den profesjonelle presse. De er stort sett nokså forskjellige fra andre publisister på nett. Det vil videre være et komplisert stykke arbeid å få andre typer organer til å slutte seg til PFU. Det er dessuten langt fra sikkert at PFU ville ønske det.

Det finnes sikkert noen andre man kunne vurdere i denne diskusjonen, men jeg vil likevel konkludere med at det ikke er noen god løsning å legge de her omtalte oppgavene til eksisterende organer. Uansett vil mandatendringene være såpass store og de oppgavene de ellers har så forskjellige at det vil lønne seg å ha en egen og ny nemnd.

10.3 Administrativ plassering

En helt annen diskusjon som særlig dukker opp dersom resultatet blir en nemnd med offentligrettslig forankring er hva slags administrativ plassering den skal ha. Med administrativ plassering tenker jeg her noe i likhet med den rollen forbrukernemndene har i forhold til Forbrukerrådet, noe som i og for seg kan variere. Også her kan en tenke seg ulike organer diskutert som for eksempel Datatilsynet. Motforestillingene her vil etter min mening være de samme som om man la hele oppgaven til Personvernnemnda.

Medietilsynet vil selvsagt også kunne vært en kandidat, men også her vil en kunne anføre at det ikke nødvendigvis er noen fordel at de holder på med innholdsvurderinger på lignende områder (eks film og videogram).

Skal en legge oppgaven til et eksisterende organ er undertegnede av den oppfatning at det kunne være Post- og teletilsynet. Post- og teletilsynet driver i svært liten grad med innholdsklager, men i høy grad med elektronisk kommunikasjon. Dette er etter min mening en fordel ikke minst fordi mange andre organer vil kunne sies å ligge for nær visse typer saker. En kunne derfor tenke seg at Post- og teletilsynet hadde samme rolle overfor en nettnemnd som den de har overfor Domeneklagenemnda, jf. domeneforskriften[27]. Denne forskriften etablerer Domeneklagenemnda og legger tilsynet med forskriften til Post- og teletilsynet, jf. forskriftens § 9. Domeneklagenemnda er ellers helt forskjellig fra den type nemnd som her diskuteres, ikke minst fordi nedslagsfeltet er smalt og begrenset til klager vedrørende rettigheter til domener på .no.

Den kanskje mest aktuelle løsningen vil være å legge nemnden administrativt under Nærings- og handelsdepartementet som er ansvarlig for ehandelsloven. Det burde imidlertid ikke være noe i veien for at en nemnd legges administrativt under Post- og teletilsynet selv om ordningen baseres i forskrift med hjemmel i ehandelsloven.

Boks 2.7

Nemnda legges administrativt under Nærings- og handelsdepartementet, alternativt den legges den under Post- og teletilsynet. Det siste vil kanskje være den mest nøytrale plassering i forhold til aktuelle særinteresser.

[27] Forskrift om domenenavn under norske landkodetoppdomener (domeneforskriften). Fastsatt ved Kronprinsreg.res. 1. august 2003 med hjemmel i lov av 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) § 7-1 og § 10-1 annet ledd. Fremmet av Samferdselsdepartementet.

11 Sammensetning og oppnevningsprosedyrer

Oppnevning av medlemmer og oppnevningsprosedyrer er viktig for å sikre et uavhengig og kompetent organ. Likeså må det stilles spørsmål om hvor mange medlemmer en nemnd skal ha.

Etter en gjennomgang av flere nemnder viser det seg å være vanlig at leder og nestleder har varamedlem. Det er også vanlig at Forbrukerrådets representanter har varamedlemmer.

I forhold til den kommende Brukerklagenemnda er det ikke klart hvor mange medlemmer den skal ha, bare at det i tillegg til leder skal være et likt antall fra forbrukersiden og næringsinteressene.

Etter undertegnedes mening er det ikke nødvendig at en nemnd som her tenkes har flere enn fem til åtte medlemmer. I Nettnemndas prøveprosjekt hadde man fem medlemmer, og jeg tror det er minimum av hva man må ha, mens Personvernnemnda har åtte medlemmer, alle med personlig varamedlemmer.

Det er videre viktig at man har regler om beslutningsdyktighet. En regel her kan være at beslutningsdyktighet foreligger dersom minst tre medlemmer er til stede, og leder eller nestleder er en av dem. Dette er en god regel fordi den sikrer fremdrift.

Når det gjelder sammensetningen er det vanlig at leder og nestleder er jurister. Det må ikke være slik, men etter undertegnedes mening er det en fordel. En nemnd som behandler klager som her bør i tillegg til juridisk kompetanse ha medie- og datafaglig kompetanse. Et av medlemmene bør også ha særlig kunnskap om bransjen. Kompetanse om barns forhold til ulike media kan også være nyttig.

Når det gjelder oppnevningsprosedyre er det mange måter det kan skje på. Forbrukernemndene ha stort sett innslag av representanter oppnevnt av de aktuelle næringer. Dette betyr selvsagt ikke at de stiller som nemndsmedlemmer med bundet mandat, men de vil nok likevel ofte sees på som partsrepresentanter.

Jeg mener det beste i denne type nemnd er å ha medlemmer som er oppnevnt i kraft av egen kompetanse og ikke som partsrepresentanter for en eller annen bransje.

Et annet spørsmål er hva slag ordning en bør ha for utpeking av nemndsmedlemmer. Domstolene gis undertiden i oppgave å peke ut nemndsledere og lignende. I forbrukerklagenemndene er det videre ofte representanter for den enkelte næring som utpeker nemndsmedlemmer.

Det er mange måter å tenke seg et nemndsmedlem utpekt på.

Følgende kunne tenkes å få utpeke medlemmer:
Sorenskriveren i Oslo
En relevant presseorganisasjon
Forbrukerrådet
En relevant akademisk institusjon/institutt
Et forvaltningsorgan (Statens medieforvaltning, Datatilsynet eller Post- og teletilsynet)

For Personvernnemndas del blir lederen og nestlederen oppnevnt av Stortinget. De øvrige fem medlemmene oppnevnes av Kongen. Sivilombudsmannen kunne også tenkes å få en utpekingsoppgave.

12 Litt om noen sammenlignbare nemnder

På en måte vil en kunne si at ingen nemnder kan sammenlignes med den type en her tenker seg. Likevel er det slik at veldig mange rettskonflikter nettopp finner sin løsning i nemnder.

Nedenfor ser vi en oversikt over kostnads – og klagebilde for noen utvalgte forbrukernemnder.

I alt finnes det et tyvetalls nemnder av denne typen. Dette kan gi en indikasjon på hva en ordning kan koste.

Forsikringsklagekontoret har 32 ansatte og kostet i 2007, 23 300 000. Forsikringsklagekontoret avsluttet 5.625 saker i 2007.[28]

Banklagenemnda har 5 ansatte og et budsjett på 5 500 000. Bankklagenemnda avga i 2007 156 uttalelser (129 i 2006). [29]

For det nå nedlagte Teletorgrådet ble det i 2005 bevilget kr 1.400.000 til Teletorgrådet som hadde én person ansatt i sekretariatet og behandlet opp i mot 150 saker i året.

Pressens faglige utvalg, PFU, behandlet i 2007 314 klager. Det er vanskelig å få noe kostnadsoverslag. Ordningen er en del av Presseforbundets virksomhet.[30]

Kostnader, sakstype og saksomfang varierer som man ser meget. Skal en nemnd fungere må

[28] Årsberetning Forsikringsklage kontoret 2007. http://www.forsikringsklagekontoret.no/assets/fkk_aarsmeld_07.pdf

[29] Årsberetning for Bankklagenemnda 2007. http://www.bankklagenemnda.no/pdf/Arsberetning%202007.pdf

[30] http://presse.no/

den fra dag én ha et sekretariat med tilstrekkelige rammer slik at man kan begynne å arbeide effektivt med en gang. Hurtighet vil være et sentralt poeng i så henseende. Dersom man ikke kan svare og treffe eventuelle vedtak fort faller mye av hensikten bort. Det vil selvsagt gå noe tid før de første saker kommer inn for nemnda, og det vil videre ta tid før saksmengden får noe omfang.

13 Veien videre

Det bør nedsettes en arbeidsgruppe som får i oppgave å meisle ut et konkret forslag til regelverk. I en slik prosess tror undertegnede det vil være lurt å ta Nettnemndas Etiske regler for Internett som et utgangspunkt. Ikke at et regelverk bør bli identisk med Etiske regler for Internett, men det kan være et godt utgangspunkt i og med at mye av det man må tenke igjennom har vært tenkt ut før. Siden etater og organisasjoner som Forbrukerrådet og IKT-Norge har engasjert seg i spørsmålet om en nemnd som dette bør de være representert i en eventuell arbeidsgruppe.

Det viktigste er at man tilstreber å lage en ordning som har tilstrekkelige ressurser fra første dag og som derfor kan arbeide hurtig.

Nemnda bør:

- Være offentligrettslig basert.
- Statlig finansiert.
- Hjemlet i ehandelsloven av 23. mai 2003 nr 35.
- Lagt administrativt til Nærings- og handelsdepartementet, alternativt Post- og teletilsynet.
- Ha mellom fem og åtte medlemmer.
- Ha retting, sletting og stengning som sanksjon.

Vedlegg 3

Betenkning om grunnlovsfesting av retten til personvern/privatliv

Alf Petter Høgberg og Njål Høstmælingen
Overlevert Personvernkommisjonen den 3. november 2008

1 Innledning – særlig om begrepene «personvern» og «privatliv»

1.1 Introduksjon

Personvernkommisjonen har i brev av 26. august 2008 gitt oss i oppdrag å «skrive en betenkning som drøfter fordeler og ulemper ved grunnlovsfesting av retten til personvern/privatliv».

«Personvern» og «privatliv» er ikke entydige størrelser i norsk språk, ei heller i norsk lovgivning eller juridisk litteratur. Før vi går inn i de drøftelsene om norsk rett, internasjonale menneskerettigheter og mulige konsekvenser av en grunnlovsregulering, vil vi i kapittel 1 avklare hva vi legger i disse begrepene. Vi vil allerede her understreke at i Personvernkommisjonens mandat til oss er de to begrepene personvern og privatliv likestilt («personvern/privatliv»).

1.2 Personvernkommisjonens mandat

Et utgangspunkt kan tas i hvordan begrepene benyttes av og for Personvernkommisjonen, siden mandatet er gitt av Personvernkommisjonen og siden vår betenkning er ment å utgjøre et vedlegg til Personvernkommisjonens sluttrapport.

I mandatet for Personvernkommisjonen (www.personvernkommisjonen.no/docs/mandat.html) heter det i punkt 1:

> «Personvern kan verte definert på ulike vis. Sentralt i omgrepet står at kvart einskilt menneske er ukrenkjeleg og har krav på respekt frå andre menneske, for eigen integritet og for fred i sitt privatliv. Personvern er såleis nært knytt til einskildindividet sitt høve til privatliv, sjølvråderett (autonomi) og sjølvutfalding. Retten til privatliv følgjer mellom anna av den europeiske menneskerettskonvensjonen (EMK) artikkel 8, og står sentralt i EU sitt personverndirektiv (95/46 EF).»

Dette utgangspunktet i mandatet er ikke helt presist. Mandatet lest snevert indikerer at personvern er noe mer enn privatliv (også inkluderende selvråderett og selvutfoldelse), men på den annen side er privatliv i internasjonal menneskerettighetssammenheng definert slik at det omfatter også disse to sistnevnte forholdene (se mer om dette nedenfor i kapittel 4). Den første presiseringen i mandatet, som knytter personvern opp mot at hvert enkelt menneske er ukrenkelig, dekkes dels av det menneskerettslige privatlivsbegrepet, men også av de mer spesifikke bestemmelsene om integritet (som i EMK artikkel 2 og 3).

Annen del av punkt 1 i mandatet trekker inn et nytt begrep, nemlig personopplysningsvern. Dette begrepet presenteres som eksempel på konflikt mellom privatliv og integritetsbeskyttelse på den ene siden og andre sentrale rettigheter på den andre:

> «Som andre grunnleggjande rettar må retten til privatliv og vernet til den einskilde sin integritet vegast opp mot andre sentrale rettar og verdiar. Retten til å hegne om personopplysningar kan til dømes komme i konflikt med retten til frie ytringar eller med samfunnet sin trong for vern mot kriminelle handlingar.»

Denne type konflikt mellom rettigheter er vanlig for mange av menneskerettighetene, for eksempel vern mot diskriminering satt opp mot ytringsfrihet. Introduksjonen av konflikt bringer oss dermed ikke nødvendigvis noe nærmere innholdet i begrepene, men det er likevel mulig å lese ut en parallellitet mellom «privatliv» og «personopplysningar» på den ene siden og «andre sentrale rettar og verdiar» og «frie ytringar» på den andre siden. Teksten lest på denne måten indikerer at personopplysninger er del av privatlivsbegrepet.

Punkt 2 i Personvernkommisjonens mandat er i all hovedsak fokusert på personopplysningsvern, både i forhold til de mer abstrakte vurderin-

gene innledningsvis og de konkrete eksemplene mot slutten av punktet.

I punkt 3 i mandatet er ordet «personvern» igjen det dominerende, men de konkrete eksemplene gir klar indikasjon på at det er personopplysningsvern – og ikke det bredere personvern – som er i fokus.

I Personvernkommisjonens mandat til oss er de to begrepene personvern og privatliv likestilt («personvern/privatliv»). I mandatet til Personvernkommisjonen er det EMK artikkel 8 som nevnes, sammen med EUs personverndirektiv. Men også integritetsvernet nevnes i mandatet.

Personvernkommisjonens mandat er ut fra det ovenstående relativt åpent i forhold til begrepsparet «personvern» og «privatliv».

1.3 Personvernkommisjonens delrapport

Personvernkommisjonen har mandat til å levere delrapporter (jf. mandatet punkt 3). Én slik rapport er levert i skrivende stund («Medier og personvern», datert 9. oktober 2008, se http://pvk.no/docs/medierogpv.pdf). Delrapporten vil kunne bidra til en presisering av begrepene gjennom synliggjøring av hva Personvernkommisjonen selv legger i begrepene.

I delrapporten forklares noen begreper i kapittel 1, hvor særlig dette sitatet er sentralt:

> «Personvernkommisjonen finner det nyttig å skille mellom begrepene ‹personvern› og ‹personopplysningsvern›. Personvern dreier seg om ivaretakelse av personlig integritet, mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse. Personopplysningsvern dreier seg om regler, retningslinjer og standarder for behandling av personopplysninger, og som har ivaretakelse av personvern som hovedformål. En personopplysning i denne sammenhengen er en opplysning som direkte eller indirekte kan knyttes til en fysisk person.»

Det skrives ikke noe mer i delrapporten om hvilket av disse to begrepene Personvernkommisjonen videre arbeider med, men det heter samme sted at kommisjonen vil i sin «sluttrapport utdype begrepene personvern og personopplysningsvern». I den videre teksten i delrapporten (særlig kapittel 2 og 3) diskuteres dels personvern i vid forstand (for eksempel satt opp mot andre rettigheter) og personopplysningsvern mer snevert, mens det i de operative anbefalingene i kapittel 4 dreies inn mot personopplysningsvern. Selv om rapportens overskrift bruker ordet personvern og ikke personopplysningsvern, er det det siste som i stor grad er i fokus.

I delrapporten behandles en lang rekke avgjørelser fra Europarådets menneskerettighetsdomstol (EMD), sammen med EMK artikkel 8 (privatliv) og 10 (ytringsfrihet). I mandatet til Personvernkommisjonen er det EMK artikkel 8 som nevnes, sammen med EUs personverndirektiv. Gjennomgangen av konvensjonsvernet i delrapporten viser at kommisjonen oppfatter personopplysningsvernet som del av EMK artikkel 8, men bidrar ut over det ikke til avklaring av det mulige skillet mellom personvern og privatliv.

Ut fra det ovenstående forstår vi begrepsbruken i delrapporten slik at personopplysningsvern er del av det større personvern, og at grensen mellom personvern og privatliv er relativt åpen.

1.4 Innlegg av Personvernkommisjonens leder

Personvernkommisjonen ble etablert 25. mai 2007, og ledes av Kjellbjørg Lunde. I foredrag på Personvernkonferansen 7. desember 2007 drøftet hun mandat og oppgaver. Innledningsvis redegjorde hun for begrepene personvern og personopplysningsvern (kapittel 1):

> «Vi snakkar gjerne om personvern og personopplysningsvern. Uttrykket personvern handlar om vern av den personlege integriteten – det at vi har krav på respekt for vårt privatliv, rett til å holde ting for oss sjølve, osb. Personopplysningsvern er ein underkategori av personvern, og handlar om normer og regler for behandling av personopplysningar.»

Avklaringen er nyttig i forhold til personopplyningsvern (det at personopplysningsvern er en underkategori av personvern), men sier mindre om grensene mellom personvern og privatliv. Noe kan kanskje trekkes ut av den andre setningen, som kan tolkes som at personvern er del av personlig integritet, og at personlig integritet igjen er del av privatliv, men dette kan for så vidt like gjerne tolkes i motsatt retning.

I den avsluttende delen av innlegget, legger Lunde vekt på personlig integritet og autonomi (kapittel 8):

> «På den eine sida meiner vi at retten til personleg integritet og autonomi er ein menneskerett, på lik linje med ytringsfridomen. På den andre side meinar vi at samfunnsoppgåver som helse, velferd, tryggleik og infrastruktur ikkje kan neglisjerast, og det finst situasjonar der omsynet

til desse må vegast opp mot, og går foran, personvernomsyn.»

Innlegget dreier i all hovedsak om personopplysningsvern, men både innledning og avslutningen inkluderer en videre arbeidsoppgave enn bare personopplysningsvern. Utsagnet er imidlertid ikke avklarende i forhold til begrepene personvern og privatliv.

1.5 Personopplysningsloven

Personopplysningsloven (lov av 14. april 2000 nr 31) bygger blant annet på NOU 1997: 19 Et bedre personvern – forslag til lov om behandling av personopplysninger. Denne offentlige utredningen ble utarbeidet i samme tidsrom som Ytringsfrihetskommisjonen, og de to kommisjonene relaterte sitt arbeid til hverandre (se mer om det nedenfor). Begrepsbruken i loven kan dermed være relevant også i vår sammenheng.

Den kommisjonen som forfattet NOU 1997: 19 skulle i henhold til mandatet i all hovedsak behandle personopplysninger (side 46-47). Personvern/privatliv i bredere forstand ble behandlet kun rent summarisk, og NOUen har lite å tilføre vår diskusjon.

Personopplysningsloven § 1 lyder:

> «Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger.
>
> Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.»

Ut fra denne lovteksten er det klart at vern av personopplysninger er del av personvern, i den forstand at personvern kan bli «krenket gjennom behandling av personopplysninger» (jf. annet ledd). I samme retning trekker annet ledd, om at «personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn».

Formålsbestemmelsen sier også noe om forholdet mellom personvern og noen av de andre begrepene som er nevnt ovenfor. «Personvernhensyn» er i henhold til annet ledd relatert til «personlig integritet» og «privatlivets fred». Teksten kan tolkes i retning av at personvernhensyn er et samlebegrep for personlig integritet og privatlivets fred, men det vil nok være å strekke teksten litt langt.

Vi leser personopplysningsloven slik at den bekrefter vårt utgangspunkt i de forrige underkapitlene, om at personopplysningsvern er del av det større personvern, men igjen bidrar ikke dette til avklaring av begrepene personvern og privatliv.

1.6 Grunnlovsforslag om privatlivets fred og personopplysninger

I grunnlovsforslag fra Venstre i 2008 om privatlivets fred og personopplysninger, brukes ulike begreper knyttet til den tematikken som denne utredningen omhandler (se dokument nr. 12: 18 for 2007-2008). I grunnlovsforslaget brukes ord som «privatlivets fred», «personopplysninger», «en privat sfære», «vern for privatlivet», «personvern», «beskyttelse av hjem» og «vern om privatsfæren». Det skilles ikke klart mellom begrepene, særlig ikke når det gjelder «personvern» og «privatliv».

Forslagsstillerne skriver at «[p]ersonvern innebærer først og fremst beskyttelse av hjem og privatsfære», og fortsetter: «Men personvern gjelder også i stor grad beskyttelse mot utilbørlig elektronisk behandling og bruk av personopplysninger».

Videre i dokumentet argumenteres det dels i forhold til personvern i vid forstand, og dels i forhold til beskyttelse av personvernopplysninger, særlig grunnet teknologisk utvikling (avsnitt 4). Stedvis trekkes det et skille mellom de to begrepene, men forslagsstillerne kobler samtidig de to begrepene. Forslagsstillerne skriver for eksempel i femte avsnitt at det i de «fleste moderne konstitusjoner [finnes] bestemmelser om vern om privatsfæren, og bestemmelser om beskyttelse av personopplysninger er på vei inn».

Når det gjelder lovhjemler, omtales dette slik i forslaget:

> «Personvernet reguleres i dag blant annet av straffelovens bestemmelser om ærekrenkelse og privatlivets rett til fred. Til dette kommer bestemmelsene i personopplysningsloven, helseregisterloven, lov om elektronisk kommunikasjon og loven om Schengen informasjonssystem (SIS).»

Denne måten å presentere lovhjemlene på, underbygger skillet mellom de to begrepene, men får samtidig frem koblinger mellom de to.

Det gis i grunnlovsforslaget også referanse til Stortingets anmodning om grunnlovsfesting av vern for privatliv i forbindelse med behandlingen av Grunnloven § 100 om ytringsfrihet, og forslagsstillerne sammenligner sitt grunnlovsforslag med

blant annet «bestemmelsene om ytrings- og informasjonsfrihet». Denne bruken av begrepet tilsvarer den tradisjonelle sammenligningen av EMK artikkel 8 med EMK artikkel 10.

Forslagsstillerne ber om to ulike grunnlovsbestemmelser, en om privatlivets fred (ny § 100a eller § 100b) og en om personopplysninger (ny § 100c) (jf. alternativ 1), eventuelt at disse slås sammen i én ny bestemmelse (alternativ 2 og 3).

Vi leser grunnlovsforslaget slik at det dreier rundt den samme delingen som vi viste i underkapittel 2.1. nedenfor, det vil si at personvern og privatliv dekker mer enn personopplysningsvern, og at grensen mellom personvern og privatliv er relativt åpen.

1.7 Ytringsfrihetskommisjonen

I arbeidet frem mot endringen av Grunnloven § 100 om ytringsfrihet i 2004, ble begrepene personvern og privatliv diskutert av Ytringsfrihetskommisjonen (NOU 1999: 27 «Ytringsfrihed bør finde sted»).

Ytringsfrihetskommisjonen tilnærmer seg begrepene fra ulike vinkler, men alt innenfor rammene av at utvalget skulle «foreta en grunnleggende gjennomtenkning av ytringsfrihetens stilling i vårt samfunn» (side 13).

Et innledende avsnitt viser hvordan Ytringsfrihetskommisjonen vurderer begrepene privatlivets fred og personvern:

> «Det er grunn til å understreke den prinsipielt viktige forskjell mellom ‹privatlivets fred› og ‹personvern›. Beskyttelsen av privatsfæren (‹privatlivets fred›) har en begrunnelse ut over personvernet, en begrunnelse som går på kollektivets eller samfunnets måte å fungere på. Konkret kan det gjelde hensynet til den offentlige samtale. Personvernet går på den annen side først og fremst på beskyttelsen av personen som offentlig person (offentlig omdømme), og nettopp ikke spesielt som privat person. Dette skille er ikke alltid observert som det bør være i diskusjonen om disse tema.» (side 29)

Denne bruken av begrepene gir mer innhold i et mulig skille mellom personvern og privatliv enn i diskusjonene i underkapitlene ovenfor. Men teksten preges i stor grad av de rammene som er satt for Ytringsfrihetskommisjonens arbeid, noe som kommer til uttrykk i de eksemplene som velges.

Det samme skillet mellom personvern og privatlivets fred gjentas annet sted i utredningen (side 140-141), men også her gir Ytringsfrihetskommisjonens mandat klare rammer for begrepsbruken:

> «Vi har imidlertid argumentert for at ‹privatlivets fred› går ut over det vi vanligvis assosierer med den vage og vide betegnelsen ‹personvern›, idet ‹privatlivets fred› ikke bare søker sin begrunnelse i individuelle interesser, men også i kollektive. Dessuten går personvernet først og fremst på den enkeltes vern som individ i offentligheten og ikke i privatsfæren.»

Personopplysningsvern berøres også av Ytringsfrihetskommisjonen, og forstås av kommisjonen som del av det større begrepet privatliv. Et eksempel er diskusjonene på side 28:

> «Det har vært en tendens i retning av å bygge ned beskyttelsen av privatlivet, både når det gjelder inngrep fra det offentlige og innsyn fra offentligheten. Det kan være gode grunner for å regulere beskyttelsen i begge tilfelle, for eksempel når det gjelder barnevern eller beskyttelse mot vold innenfor familien, eller når det gjelder visse deler av særlig offentlige personers mer private anliggender. Adskillig mer betenkelig er utviklingen av den offentlige registrering, ikke minst når det gjelder tendensen til å koble forskjellige dataarkiver. Her kan det nesten se ut som vi glir dumsnille inn i ‹the brave new world›.»

I vår sammenheng er Ytringsfrihetskommisjonens kommentarer om grunnlovsbeskyttelse av privatlivets fred særlig interessante (side 113):

> «Det er grunn til å påpeke at den norske Grunnlov ikke har en alminnelig bestemmelse om privatlivets fred ut over § 102s forbud mot «Hus-Inkvisitioner». En slik allmenn bestemmelse finner vi i flere grunnlover, blant annet i den danske grunnlovs § 72 og i EMK art. 8. Disse paragrafer gir en ekstra beskyttelse for ytringsfriheten i privatsfæren i forhold til den offentlige sfære. I norsk rett er dette et noe uklart område […]. Ytringsfrihetskommisjonen er av den oppfatning at det beste ville vært om den norske Grunnlov hadde hatt en paragraf om privatlivets fred. […] Privatlivets fred omfatter langt mer enn bare ytringsfrihet. Et forslag til en egen grunnlovsparagraf om privatlivets fred ville krevet en egen utredning og gått ut over kommisjonens mandat. Kommisjonen har derfor begrenset seg til å legge forslaget om forbud mot forhåndssensur av private ytringer, med tilhørende unntak, inn i ytringsfrihetsparagrafen.»

Ytringsfrihetskommisjonen gjentar i dette avsnittet at deres forståelse av personvern og privatlivets fred er diskutert med ytringsfrihet som ramme. Kommisjonen understreker også det opplagte, at privatlivets fred favner langt mer enn ytringsfrihet. Viktigere er da denne kommisjonens bruk av ordet privatlivets fred i første og annen punktum: her kobles privatlivets fred med EMK artikkel 8, som favner langt bredere enn det kommisjonen legger til grunn i den øvrige teksten.

Av fremstillingen ovenfor fremgår det et skille mellom personvern og privatlivets fred når det gjelder den private sfære, hvor personvern blir forstått som en del av privatlivets fred. Samtidig er det klart at personopplysningsvern er noe mindre enn personvern. Ytringsfrihetskommisjonen er samtidig tydelig på at begrepsavklaringene skjer innen det rommet de var satt til å utrede, nemlig ytringsfrihet.

1.8 Nye Grunnloven § 100

I Stortinget ble Ytringsfrihetskommisjonens utredning drøftet av Kontroll- og konstitusjonskomiteen i Innst. S. nr. 270 (2003-2004) (via St.meld. nr. 26 (2003-2004)). I store trekk adopterer Kontroll- og konstitusjonskomiteen den begrepsbruken som Ytringsfrihetskommisjonen la til grunn. I Kontroll- og konstitusjonskomiteens sammendrag av stortingsmeldingen heter det (kapittel 4.2):

> «Ytringsfrihetskommisjonen har drøftet betydningen av å skille mellom den offentlige og private sfære i flere sammenhenger. Det trekkes et prinsipielt skille mellom ‹personvernet› og ‹privatlivets fred›. […] Med personvernet tenker kommisjonen først og fremst på beskyttelsen av personen som offentlig person (offentlig omdømme). Vernet om ære og verdighet er en sentral del av personvernet. […] Med beskyttelse av privatlivets fred eller beskyttelse av privatsfæren tenker kommisjonen på tre forhold».

De tre forholdene som komiteen viser til, er vern mot inngrep fra det offentlige, skjerming mot innsyn og vern mot offentliggjøring av private forhold.

Departementets forståelse av lovgrunnlagene presenteres slik av Kontroll- og konstitusjonskomiteen i innstillingen:

> «Grunnloven har ingen regler som uttrykkelig verner retten til privatlivets fred. En viss beskyttelse følger av Grunnloven § 102 […]. For øvrig gir straffeloven § 390 vern mot å ‹krenke[r] privatlivets fred ved å gi offentlig meddelelse om personlige eller huslige forhold›. De hensyn som ligger til grunn for bestemmelsen, må avveies mot hensynet til ytringsfriheten. Privatlivets fred er beskyttet av EMK artikkel 8. Bestemmelsen retter seg først og fremst mot inngrep fra statlige myndigheter i den fysiske og psykiske integritet. Overvåking og enkelte spørsmål om misbruk ved registrering av personopplysninger faller også inn under bestemmelsen.»

Gjennomgangen av lovgrunnlag, og da særlig EMK artikkel 8, viser at begrepet privatlivets fred kan strekkes ganske langt. Den eneste reelle grensen som departementet her trekker (slik Kontroll- og konstitusjonskomiteen har forstått det), er i forhold til vern mot krenkelser fra andre private. Det er samtidig viktig at begrepet privatlivets fred, som presenteres i første setning, uttrykkelig forankres i EMK artikkel 8 i femte setning i sitatet ovenfor («Privatlivets fred er beskyttet av EMK artikkel 8»).

Et interessant innspill i forhold til begrepsbruk kommer fra SV (kapittel 4.2.1):

> «Men privatlivets fred er, etter komiteens medlemmer fra Sosialistisk Venstrepartis mening, ikke alltid synonymt med familielivets fred. Mange kvinner er blitt utsatt for vold fra samboer eller ektefelle uten at det er blitt grepet inn fra det offentliges side, og begrunnelsen har vært beskyttelse av familielivets fred.»

Dette innspillet kan tyde på at SV her ønsker å legge noe mer i privatlivets fred enn resten av komiteen, i den forstand at begrepet også omfatter familielivets fred, men dette kan også leses i motsatt retning, om at familielivets fred ikke favnes av privatlivets fred. Innspillet kan imidlertid like gjerne være en reaksjon på departementets presisering av ansvarsforhold (og ikke materiell rekkevidde) (jf. kapittel 4.2):

> «Det er noe mer tvilsomt i hvilken utstrekning artikkel 8 første ledd gir vern mot krenkelser fra andre private. Trolig har statene en viss, begrenset forpliktelse til gjennom lovgivning og domstoler å sørge for at private ikke krenker hverandres privatliv.»

Kontroll- og konstitusjonskomiteen drøfter behovet for eventuell grunnlovsfesting av privatlivets fred, uten at begrepsbruken bidrar til ytterligere presisering. Komiteen konkluderer slik i kapittel 4.2.1:

«Stortinget ber Regjeringen utrede vernet av privatlivets fred, herunder spørsmålet om mulige utforminger av en eventuell grunnlovsfesting.»

Innstillingen debatteres i Stortinget 30. september 2004. I disse diskusjonene benyttes ikke begrepet personopplysningsvern. Begrepene personvern og privatliv nevnes, men uten at det trekkes klare skiller mellom de to. SVs dissenterende presisering i komitéinnstillingen knyttet til vold i hjemmet, blir ikke direkte tatt opp igjen i debatten. Igjen er ytringsfrihet rammene for diskusjonene og begrepsbruken, vist for eksempel i innlegg av Berit Brørby (A):

«Vern av privatlivets fred er et annet viktig område for debatten om ytringsfriheten. Jeg er glad for at en samlet komité står bak henstillingen til Regjeringen om å utrede hvorvidt det er behov for en egen bestemmelse om dette i Grunnloven.»

Vi forstår Stortingets diskusjon slik at det ikke trekkes noe klart skille mellom personvern og privatliv, og samtidig at privatlivets fred i store trekk er sammenfallende med, eller i alle fall inkludert i, EMK artikkel 8.

1.9 SOU 2008: 3 – Skyddet för den personliga integriteten

Den svenske Integrietetsskyddkomittén avga sin sluttbetenkning «Skyddet för den personliga integriteten» som SOU 2008: 3. Komiteen har hatt et oppdrag som i stor grad er sammenfallende med Personvernkommisjonen. I sin sammenfatning skriver komiteen at de har «haft i uppdrag att kartlägga och analysera skyddet i lagstiftningen för den personliga integriteten samt överväga om detta skydd behöver kompletteras» (side 13).

Komiteens mandat behandler eksplisitt begrepet «personlig integritet» (side 340-341). Viktigst her er de innledende skillene som trekkes:

«I olika utredningar […] har man med utgångspunkt bl.a. i de grundläggande fri- och rättigheterna i regeringsformens andra kapitel försökt ringa in begreppet genom att skilja mellan den rumsliga integriteten (hemfriden), den materiella integriteten (egendomsskyddet), den kroppsliga integriteten (skydd för liv och hälsa, mot ingrepp i eller mot kroppen), den personliga integriteten i fysisk mening (skyddet för den personliga friheten och rörelsefriheten) och den personliga integriteten i ideell mening (skyddet för privatlivet och för personligheten inklusive den privata ekonomin).»

Komiteen legger innledningsvis en tilsvarende bred begrepsforståelse til grunn, i hovedsak sammenfallende med EMK artikkel 8 (jf. også oppramsingen i mandatet inntatt på side 341). Men i forbindelse med gjennomgangen av gjeldende rett, presiserer komiteen sin begrepsforståelse slik (side 74-75):

«Kommittén har emellertid avgränsat sitt arbete till att i huvudsak omfatta den personliga integriteten i ideell mening. Av intresse i detta sammanhang är således framför allt skyddet för privatlivet och skyddet för hem och korrespondens. Utanför kommitténs arbete faller däremot i huvudsak det skydd som artikeln ger för den fysiska integriteten, för sexuella relationer och för familjelivet. Inte heller de sociala rättigheter eller utlänningars rättigheter som anses följa av artikeln omfattas av kommitténs arbete. I centrum för kommitténs överväganden står frågor som hör samman med informationen om den enskilde och den enskildes rätt att få vara i fred. Av intresse är särskilt hur den personliga integriteten skyddas i samband med insamling och offentliggörande av uppgifter och hur identifieringsdata så som namn och bild skyddas.»

Den svenske utredningen gir ikke i seg selv føringer på vårt arbeide, men viser at begrepene personvern og privatliv kan tolkes i en vid og en snever forstand.

1.10 Oppsummering

Forholdet mellom begrepene «personvern» og «privatliv» er ikke entydig og klart, noe også Personvernkommisjonens mandat og arbeid viser. En tilsvarende uklarhet følger av personopplysingsloven, grunnlovsforslag om privatlivets fred og personopplysninger, Ytringsfrihetskommisjonens utredning og Stortingets behandling av Grunnloven § 100. Flere av de kildene som er beskrevet ovenfor, har vært relatert til ytringsfrihet. Begrepsbruken og eksemplene er dermed også preget av de rammene som ytringsfriheten setter.

I det følgende vil vi arbeide ut fra en forståelse om at personopplysningsvern omfattes av begrepene personvern og privatliv. Videre finner vi det ikke nødvendig å trekke noe klart skille mellom personvern og privatliv. Selv om det ikke skulle være full identitet mellom begrepenes dekningsområder, er det uansett store fellesområder. Vi vil

i det følgende legge til grunn det innholdet som særlig følger av EMK artikkel 8, men vil også trekke inn eksempler knyttet til en bredere forståelse av fysisk og psykisk integritetsvern.

2 Om vernet av personvern/privatliv etter «intern» norsk rett

2.1 Innledning

Vårt rettssystem inneholder en rekke bestemmelser med betydning for borgernes personvern/privatliv. Det dreier seg til dels om rettsregler som direkte har som siktemål å sikre personvern/privatliv, og til dels om regler som i bestemte situasjoner rent faktisk styrker borgernes personvern/privatliv.

Som nevnt under punkt 1.10 ovenfor, legges det i denne betenkningen til grunn vidt begrep «personvern»/«privatliv»; et begrep som bl.a. omfatter delvis overlappende underkategorier som personlighetens rettsvern, privatlivets fred og personopplysningsvern. I det følgende skal fokus rettes mot de eksisterende regler som er av betydning for et slikt vern.

Siden problemstillingen for vår betenkning har et rettskildefokus, vil også den foreliggende fremstillingen ha et rettskildefokus. Vi tredeler den internrettslige reguleringen i (1) den grunnlovsmessige reguleringen, (2) regulering i formell lov og (3) regulering gjennom ulovfestede prinsipper, praksis og reelle hensyn. Den fremstillingsmessige rekkefølgen er ikke ment å si noe om faktorenes rolle og vekt. Eksempelvis spiller legalitetsprinsippet (som hører til den kategori som behandles til sist) en meget viktig rolle i praksis, og det har stor gjennomslagskraft i møte med argumenter avledet fra andre faktorer.

2.2 Den grunnlovsmessige reguleringen

2.2.1 Generelt

Grunnlovens vern av personverninteressene er høyst ufullstendig og fremstår som temmelig tilfeldig. Det er kun Grunnloven §§ 100 fjerde ledd og 102 som direkte sikrer borgernes personvern. Grunnloven § 100 innebærer dessuten en type negativ regulering av personvernet. I tillegg har i Grunnloven § 110 c en generell fanebestemmelse som pålegger statens myndigheter å respektere og sikre menneskerettighetene. Enkelte av Grunnlovens øvrige bestemmelser vil imidlertid beskytte personverninteresser når de anvendes i bestemte kontekster. Eksempler på slike bestemmelser er Grunnloven §§ 2, 96, 97, 99, 104, 105 og 110 b.

2.2.2 Det direkte vernet: Grunnloven §§ 100.4.2 og 102

Grunnloven § 100 fjerde ledd, annet punktum sikrer borgerne mot brevsensur og lyder: «Brevcensur kan ei sættes i Værk uden i Anstalter.» Bestemmelsen har en side både mot ytringsfriheten og personvernet/privatlivet. For den brevskrivende innebærer det at noen eventuelt holder tilbake ens budskap et opplagt brudd på ytringsfriheten. Det å gripe inn i den private kommunikasjonen, i verste fall etter gjennomlesning av budskapet, innebærer imidlertid også et inngrep i både avsenders og mottagers personvern/privatliv. Denne siden av bestemmelsen har imidlertid bare i meget begrenset grad vært gjenstand for debatt. I forkant av endringen av Grunnloven § 100, sto debatten i forarbeidene særlig om brevsensur kun skulle kunne iverksettes etter særlig tillatelse fra domstol. Dette ble forkastet med den begrunnelse at et «slikt krav ville skape særlige problemer for straffegjennomføringen som ikke står i rimelig forhold til den styrkingen av ytringsfriheten som oppnås» (St.meld. nr. 26 (2003-2004), s. 133). Hensynet til personvernet/privatlivet ble i denne sammenhengen ikke drøftet, noe som muligens reflekterer at det er svak tradisjon for å sikre denne typen menneskerettigheter for personer plassert i anstalter. For alle andre borgere er imidlertid denne retten til å være fri fra forhåndssensur sikret et absolutt grunnlovsvern.

Grunnloven § 102 sikrer borgerne mot såkalte husinkvisisjoner og lyder: «Hus-Inkvisitioner maa ikke finde Sted, uden i kriminelle Tilfælde.» Bestemmelsen sikrer borgerne mot vilkårlige undersøkelser for å bringe på det rene om noe kriminelt har foregått eller foregår. Det er antatt at bestemmelsen skal tolkes i samsvar med EMK art. 8 og SP art. 17 om respekt for hjem og privatliv, jf. Høstmælingen: Internasjonale menneskerettigheter (2004, s. 215-218). Bestemmelsen ble av lovgiver imidlertid ikke ansett som en hindring for å foreta romavlytting i forebyggende øyemed, jf. nedenfor i punkt 4.6.

2.2.3 Den negative reguleringen i Grunnloven § 100

Grunnloven § 100 inneholder i tillegg til 4. ledd, 2. punktum, en type negativ regulering av personvernet/privatliv. Med negativ regulering menes

en regulering som ikke sier hva som er vernet, men hva som ikke kan være vernet. I den grad Grunnloven § 100 måtte stride mot hensyn til personvern/privatliv, vil hensynene til personvern/privatliv måtte vike.

Det er i utgangspunktet intet spesielt med den måten man foretar en type negativ regulering på i Grunnloven § 100. Ser en på bestemmelsens forarbeider, fremkommer det imidlertid at ytringsfrihetsinteressene i Grunnloven § 100 forutsettes ikke å kollidere med hensynet til privatlivets fred ettersom disse påstås å befinne seg i to ulike «sfærer»; mens ytringsfriheten og personvernet påstås å referere seg til den offentlige sfære, påstås privatlivets fred å referere seg til den «private sfæren eller intimsfæren», jf. eksempelvis NOU 1999: 27, s. 28. Skillet mellom disse sfærene har vist seg å være uholdbart som beskrivelse av rettighetenes funksjonsmøte, og legges heller ikke til grunn i nyere praksis og teori (jf. nedenfor i punktene 4.2 og 4.3). Dette innebærer at den negative reguleringen ikke fungerer etter sine forutsetninger. Den tilsynelatende forutsetningen om ytringsfrihetens forkjørsrett i forhold til privatlivets fred, viser seg ved undersøkelse av forarbeidene ikke å være noe annet og mer enn en forutsetning om at de to rettighetene aldri vil kollidere da de befinner seg i hver sin sfære.

2.2.4 Særskilt personvern gjennom Grunnloven § 110 c?

Grunnloven § 110 c lyder:

> «Det paaligger Statens Myndigheder at respektere og sikre Menneskerettighederne. Nærmere Bestemmelser om Gjennomførelsen af Traktater herom fastsættes ved Lov.»

Bestemmelsen er tradisjonelt oppfattet som en utpreget symbolbestemmelse som forutsetter at de enkelte rettighetene sikres gjennom inkorporasjon eller transformasjon. Bestemmelsen prioriterer heller ingen konvensjoner eller rettigheter fremfor andre. Grunnloven § 110 c spiller like fullt en rolle i ivaretakelsen av de enkelte menneskerettigheter i norsk rett, herunder personvernrettighetene, men mest gjennom menneskerettsloven som ble vedtatt med grunnlag i § 110 c annet ledd (og siden menneskerettsloven inkorporerer EMK artikkel 8 og SP artikkel 17 i norsk rett, vil vi her ha et tilfelle av nær full regulering av personvern/privatliv). Bestemmelsen utgjør en retningslinje for rettsanvendelsen i domstoler og forvaltning.

Det kan selvsagt spørres om ikke funksjonen i så henseende er av mer pedagogisk enn reell art, all den tid presumpsjonsprinsippet uansett gjelder. Når det gjelder presumpsjonsprinsippets første effekt – at man velger den løsningen som harmonerer best med folkerettens løsning i tilfeller der den interne rett isolert sett er uklar – vil ikke Grunnloven § 110 c kunne sies å ha noen betydning for rettsanvendelsen på siden av presumpsjonsprinsippet. Når det gjelder presumpsjonsprinsippets annen effekt – at man i tilfeller der norsk rett isolert sett er klar, men i strid med folkeretten, skal forsøke å harmonisere den interne retts løsning med folkeretten så lenge dette lar seg forsvare etter alminnelige rettskildeprinsipper – er det mer uklart om Grunnloven § 110 c kan spille en selvstendig rolle på siden av presumpsjonsprinsippet. Enkelte har hevdet at Grunnloven § 110 c representerer en kodifisering av presumpsjonsprinsippet på menneskerettighetenes område. Etter vår oppfatning er det ikke naturlig å foreta en slik kobling mellom de to elementene i vårt rettsystem, selv om effekten av dem i visse tilfeller kan være sammenfallende.

Det har videre blitt hevdet at Grunnloven § 110 c utgjør en skranke for myndighetenes atferd, slik at det ikke er adgang til å føre en politikk i strid med bestemmelsen (se eksempelvis Borvik: Personvern og ytringsfridom (2008, s. 28) med videre henvisninger). Det er lite tenkelig at myndighetene i praksis skulle føre en politikk som eksplisitt er i strid med bestemmelsen, men det er like fullt urealistisk å tro at bestemmelsen skulle legge rettslige bånd på den politikk som til enhver tid føres. I forlengelsen av denne påståtte «rammevirkningen» av Grunnloven § 110 c, har det vært hevdet at bestemmelsen gir grunnlag for prøvelse av grunnlovsmessighet og tilsidesettelse av formelle lover (Borvik 2008, s. 30). Også et slikt synspunkt går etter vårt syn for vidt, og er uansett ikke særlig realistisk.

2.2.5 Styrking av personvern/privatliv som kontekstavhengig sekundærvirkning; Grunnloven §§ 2, 96, 97, 99, 104, 105 og 110 b

En rekke bestemmelser i Grunnloven har som primæroppgave å beskytte eller ivareta en verdi som er noe annet og mer enn personvern/privatliv. Ser en nærmere på disse bestemmelsenes anvendelse i ulike kontekster, vil hensyn til personvern/privatliv rent faktisk nyte beskyttelse av bestemmelsen.

Et eksempel i denne forbindelse er Grunnloven § 97, som er en generell bestemmelse om at ingen lov må gis tilbakevirkende kraft. Begrunnelsen for bestemmelsen generelt kan ikke søkes i hensyn til personvern/privatliv. Like fullt er det på det rene at visse effekter av bestemmelsen ville kunne innebære beskyttelse av disse hensynene. Mens for eksempel sæddonorer tidligere hadde krav på full anonymitet, ble regelen endret ved vedtakelsen av bioteknologiloven § 2-7, hvor det fremgår at den «som er født etter assistert befruktning ved hjelp av donorsæd har ved fylte 18 år rett til å få opplysninger om sædgivers identitet». For sædgiver innebærer denne nye tilstanden en type svekkelse av privatlivets fred, noe som innebærer at bestemmelsen ikke kan gis tilbakevirkende kraft, jf. Grunnloven § 97. I forarbeidene til loven heter det således at «[b]estemmelsen har ikke tilbakevirkende kraft, og vil gjelde barn som er unnfanget etter at denne loven har trådt i kraft.» (Ot.prp. nr. 64 (2002-2003), s. 129)

Andre bestemmelser som i visse relasjoner eller under visse omstendigheter i større eller mindre utstrekning også verner personverninteresser og -hensyn, herunder hensynet til privatlivets fred, er Grunnloven §§ 2.2 («Alle Indvaanere af Riget have fri Religionsøvelse»), 96 («Pinligt Forhør maa ikke finde Sted»), 99 (som verner borgerne mot uhjemlet pågripelse og fengsling), 104 («Jord og Boslod kan i intet Tilfælde forbrydes»), 105 («Fordrer Statens Tarv, at Nogen maa afgive sin rørlige eller urørlige Eiendom til offentlig Brug, saa bør han have fuld Erstatning af Statskassen») og 110 b (retten til et sunt naturmiljø). Ettersom disse bestemmelsene ikke er satt til å verne personvernhensyn, men kun berører slike hensyn som en type sekundærvirkning i visse kontekster, kommer vi heller ikke til å forfølge bestemmelsene videre.

2.3 Regulering i formell lov

Det er en myriade av bestemmelser med betydning for personvern/privatliv i våre formelle lover. Bestemmelsene gjenfinnes i ulike lover og har ikke blitt til planmessig (ut fra et personvern/privatlivsperspektiv). Sett under ett fremstår reguleringen som relativt tilfeldig og utpreget kasuistisk.

Som for Grunnloven kan det sondres mellom bestemmelser som direkte tar sikte på positiv regulering av personvern/privatliv, og bestemmelser som i bestemte kontekster rent faktisk innebærer normering med betydning for personvern/privatliv. Og i tillegg til disse bestemmelsene har vi inkorporasjonslover som innebærer at internasjonale reguleringer av personvern/privatliv gis virkning i norsk rett. Vår viktigste inkorporasjonslov med virkning for personvern/privatliv, er menneskerettsloven (lov av 21. mai 1999 nr. 20). Denne loven inkorporerer privatlivsbestemmelsene i EMK artikkel 8 og SP artikkel 17, i tillegg til mer detaljerte og smalere bestemmelser om fysisk og psykisk integritet.

Eksempler på lover og bestemmelser som har beskyttelse av personverninteresser som direkte formål, er personopplysningsloven (lov av 14. april 2000 nr. 31 om behandling av personopplysninger), helseregisterloven (lov av 18. mai 2001 nr. 24 om helseregistre og behandling av helseopplysninger), straffeloven (lov av 22. mai 1902 nr. 10) §§ 390 (Krenkelse av privatlivets fred ved å «gi offentlig meddelelse om personlige eller huslige forhold»), 390 a (fredskrenkelser ved skremmende eller plagsom opptreden), 247 (subjektiv ærekrenkelse), 247 (objektiv ærekrenkelse) og åndsverkloven (lov 12. mai 1961 nr. 2) § 45 c (retten til eget bilde). Disse bestemmelsene har referanse til de fleste av personvernbegrepets elementer: Personopplysningsvern, personlighetens rettsvern og privatlivets fred.

Eksempler på bestemmelser der vernet at personverninteresser er situasjonsbestemt, er straffeloven §§ 135 a (diskriminerende og hatefulle ytringer), 431 (redaktøransvaret), 147 (innbrudd), 355 (uberettiget opphold på fremmed eiendom) og ekteskapsloven § 32 (rådighet over felles bolig). En viktig gruppe av lovbestemmelser som ivaretar personvernhensyn, er regler om taushetsplikt inntatt i en rekke lover, jf. eksempelvis forvaltningsloven (lov av 10. februar 1967) § 13 og domstolsloven (lov av 13. august 1915 nr. 5) § 227. Også en rekke andre lover har en side mot personvern/privatliv. Eksempler i denne forbindelse er abortloven (lov av 13. juni 1975 nr. 50), barneloven (lov av 8. april 1981 nr. 7), barnevernloven (lov av 17. juli 1992 nr. 100), utlendingsloven (lov av 24. juni 1988 nr. 64) og forurensningsloven (lov av 13. mars 1981 nr. 6). Selv om det ikke er noen sterk norsk tradisjon for å se på alle disse lover som regelsett som regulerer personvern/privatliv, er det like fullt et faktum at EMK artikkel 8 regulerer deler av disse lovers virkningsområde, jf. nedenfor i punkt 3.

I nyere bestemmelser som tar sikte på beskyttelse av personvernhensyn, vil lovgivningen bl.a. ha som formål å implementere de relevante EU-direktivene på området. Eksempler på direktiver

som på dette vis påvirker beskyttelsen av personverninteresser ved å innvirke på lovenes innhold, er direktivet om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (95/46/EF) og direktivet om behandling av personopplysning og beskyttelse av privatlivets fred i den elektroniske kommunikasjonssektor (2002/31/EF).

2.4 Regulering gjennom ulovfestede prinsipper, praksis og reelle hensyn

Som nevnt ovenfor i punkt 2.3, fremstår lovreguleringen av personvern/privatliv som relativt tilfeldig og utpreget kasuistisk. Dette innebærer et rikt samspill med argumenter som kan tilbakeføres til ulovfestede prinsipper, praksis og reelle hensyn.

Grensen mellom de tre størrelsene er ikke skarp. Med prinsipper mener vi materielle rettssetninger på høyt generalitetsnivå som må antas å bli respektert selv om de ikke er kodifisert gjennom vedtatt regelverk, eventuelt uavhengig av på hvilken måte de er kodifisert. Det er ikke sjelden et nært samspill mellom slike prinsipper og rettspraksis: Prinsippene har gjerne støtte i rettspraksis, og fremtrer støtten som dekkende for de fleste elementer av prinsippet, vil enkelte anse prinsippet som avledet av rettspraksis. På den annen side er det jo en grunn til at rettspraksis ble som den ble, og en nærliggende grunn er nettopp at dommerne la til grunn et ulovfestet, generelt prinsipp.

Reelle hensyn er navn på ulike godhetsbetraktninger. Dersom reelle hensyn brukes på et høyt normativt generalitetsnivå, kan det være på sin plass å snakke om prinsipper. Dersom argumentasjonen er sterkt preget av den konkrete saken og de hensynene som i den gjør seg gjeldende, fremkommer det som mindre naturlig å snakke om reelle hensyn.

Det kanskje viktigste ulovfestede prinsippet med betydning for borgernes personvern/privatliv, er legalitetsprinsippet. Det følger av legalitetsprinsippet i sin klassiske formulering at myndighetene ikke kan gripe inn i borgernes rettsfære uten hjemmel i formell lov. I nyere teori har legalitetsprisnippet blitt nyformulert innenfor en bredere kompetanselære. Det heter innenfor denne læren at kompetanse er som hovedregel en nødvendig betingelse for enhver gyldig normeringshandling, og at hjemmel i formell lov er nødvendig dersom ikke annet kompetansegrunnlag foreligger. En styrke med denne nyformuleringen er at den retter seg mot enhver som ønsker å foreta et normeringsinngrep mot en annen. Svakheten med nyformuleringen er at legalitetsprinsippet i denne skikkelsen kun retter seg mot normeringshandlinger, mens de inngripende faktiske handlinger overlates til det såkalte lex superior-prinsippet. En konsekvens av dette, er at man må operere med usanksjonerte, uskrevne forbud mot en rekke handlinger på siden av legalitetsprinsippet, noe som fremtrer som unødig oppkonstruert og formalistisk.

Det er imidlertid uansett ingen tvil om at enhver som skal foreta et faktisk eller rettslig inngrep overfor andre må kunne vise til et grunnlag for inngrepet. Vi kaller dette prinsippet for det utvidede legalitetsprinsippet. Dette utvidede legalitetsprinsippet – som har solid støtte i rettspraksis – sikrer vesentlige bestanddeler av retten til personvern/privatliv.

Ulovfestede prinsipper, rettspraksis og reelle hensyn spiller etter gjeldende rett også ved siden av legalitetsprinsippet en vesentlig rolle når de eksisterende rettsregler om personvern/privatliv skal tolkes og anvendes. Det er særlig som supplement til lovhjemlene at generelle rettsprinsipper, rettspraksis og reelle hensyn spiller en rolle. Det hender like fullt at denne ulovfestede argumentasjonsstørrelsen spiller en selvstendig rolle som grunnlag for rettsikkerhetssynspunkter som får avgjørende betydning for fastleggingen av gjeldende rett. Både Rt. 1896, s. 530 (Aars) og Rt. 1952, s. 1217 (To mistenkelige personer) er klassiske eksempler på dette. Fra nyere tid kan nevnes bevisavskjæringspraksis, der det har blitt oppstilt bevisføringsforbud dersom personvernhensyn har blitt ansett krenket og en eventuell bevisføring har blitt ansett å medføre en ny krenkelse av personvernet. Selv om det stadig eksisterer et vesentlig ulovfestet vern av personvern/privatliv, vil antakelig betydningen av disse kunne vise seg å bli mindre i fremtiden uten grunnlovsendring. Dette skyldes til dels en stadig voksende lovgivning, og til dels den nye ordlyden i Grunnloven 100 annet ledd, der det forutsettes særlig lovhjemmel for visse innskrenkninger i ytringsfriheten.

3 Det konvensjonsbaserte vernet, særlig EMK artikkel 8

3.1 Oversikt og begrepsbruk

Personvern/privatliv reguleres av flere ulike menneskerettighetskonvensjoner, og av flere bestem-

melser innen disse konvensjonene. Viktigst er bestemmelsen om retten til respekt for privatliv i EMK artikkel 8 og FNs konvensjon om sivile og politiske rettigheter (SP) artikkel 17. Bestemmelsene er i det vesentlige overlappende. Begge disse konvensjonene er gjort til del av norsk lov gjennom menneskerettsloven av 1999. Siden EMK er den som hyppigst anvendes ved norske domstoler, og siden EMD har kompetanse til å avsi folkerettslig bindende dommer i individklagesaker, rettes fokus i denne fremstillingen på EMK artikkel 8.

EMK artikkel 8 har som overskrift «Right to respect for private and family life», og lyder slik i norsk oversettelse (jf. vedlegg 2 til menneskerettsloven av 1999):

> «Artikkel 8 Retten til respekt for privatliv og familieliv
>
> 1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.
>
> 2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.»

Artikkel 8 er konstruert på en måte som først oppstiller selve rettigheten, mens inngrepshjemmelen følger av annet ledd. Dersom et tiltak er et inngrep i for eksempel retten til privatliv, vil inngrepet kunne rettferdiggjøres dersom vilkårene i annet ledd er oppfylt. Lignende systematikk finner vi for eksempel i EMK artikkel 10 om ytringsfrihet, gjenspeilet også i den reviderte Grunnloven § 100. Hovedpoenget med EMK artikkel 8 er å gi individene rett til selv å råde over seg og sitt, uten innblanding utenfra (integritetsperspektivet). I dag er det klart at retten inkluderer også det å forholde seg til andre, og å utvikle sin egen personlighet (se for eksempel saken Christine Goodwin mot Storbritannia av 11. juli 2002 (storkammer), avsnitt 90).

Ser en hen til et mer abstrakt begrep, er det klart at vi ikke har noe fullt ut dekkende ord på norsk, jf. diskusjonene i kapittel 2 ovenfor, men begrepene personvern, privatliv og privatlivets fred favnes alle av EMK artikkel 8. I norsk generell menneskerettighetslitteratur defineres bestemmelsen konkret gjennom eksempler, ikke gjennom en begrepsavklaring.

I engelskspråklige fremstillinger omtales SP artikkel 17 og EMK artikkel 8 ofte under overskriften «private life» og «privacy». Samtidig er det klart at bestemmelsene favner mer enn hva som legges i en tradisjonell «private life» eller «privacy»-betraktning. Typisk omfattes «personal autonomy, personal privacy, personal identity, personal integrity, personal development, personal identification and similar concepts linked to the individual notion of personhood» (Pieter van Dijk et al (eds.), Theory and Practice of the European Convention on Human Rights, Fourth Edition, Intersentia, Antwerpen, 2006, side 665). Det heter gjerne at «the right to privacy protects that particular area of individual existence and autonomy that does not touch upon the sphere of liberty and privacy of others» (Manfred Nowak, U.N. Covenant on Civil and Political Rights CCPR Commentary, Second Edition, Engel Verlag, Kehl, 2005, side 385). Andre forfattere tar en mer pragmatisk tilnærming, hvor en forfatter kort slår fast: «There is no single or embracing concept contained in Article 8, the issues which have arisen under Article 8 need to be classified under a number of headings» (Clare Ovey and Robin C.A. White, Jacobs & White The European Convention on Human Rights, Fourth Edition, Oxford University Press, Oxford, 2006, side 242). Linjer trekkes gjerne til filosofen John Stuart Mills skrift «On Liberty».

EMD har tilnærmet seg begrepet «private life» på denne måten (Niemietz mot Tyskland 1992, avsnitt 29):

> "The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of ‹private life›. However, it would be too restrictive to limit the notion to an ‹inner circle› in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings."

Rekkevidden av begrepene i artikkel 8 første ledd lar seg ikke beskrive helt presist. Ordene som benyttes, særlig ordet privatliv, er mer å regne for sekkebetegnelser enn presise begrep. Det er likevel klart nok at også denne bestemmelsen har en kjerne og en yttergrense, men det kan være mer fruktbart å avklare rekkevidden gjennom å se hva som er blitt dekket i praksis, heller enn å søke å finne en løsning gjennom ren ordfortolkning, slik vi gjør i underkapitlet rett nedenfor. Samtidig favner EMK artikkel 8 mange av de andre bestem-

melsene i EMK, som ytringsfrihet, trosfrihet, samvittighetsfrihet, utdanning, personlig sikkerhet og frihet, tortur, mishandling og liv. EMK artikkel 8 får anvendelse på mange områder også utenfor denne gråsonen i forhold til resten av konvensjonsvernet. Dette omfatter også områder som ikke var påtenkt da konvensjonen ble utarbeidet, som for eksempel transseksuelles rettigheter.

Hvilke av de fire begrepene (privatliv, familieliv, hjem og korrespondanse) et forhold hører inn under, er ikke avgjørende, og EMD er ikke alltid like presis her. I noen tilfeller er flere alternativer aktuelle. Seksualitet kan kanskje like gjerne dekkes av privatliv som familieliv, og avlytting er relevant både i forhold til korrespondanse, hjem og privatliv. De fire begrepene oppfattes som innbyrdes styrkende, men med hovedvekt på privatlivssiden. Det sies gjerne at de fire delene sammen bygger et overordnet privatlivsbegrep.

Den innledende formuleringen «right to respect for» i EMK artikkel 8 avviker fra mange av de andre bestemmelsene i konvensjonene, som gjerne gir en mer ubetinget rett, for eksempel til frihet og personlig sikkerhet. Ordene er i hovedsak valgt for å hindre en ubetinget positiv forpliktelse knyttet til rettighetene, for eksempel som at myndighetene hadde en plikt til å skaffe individer bolig. (Tilsvarende følger av EMK artikkel 12, EMK TP7 artikkel 5 og SP artikkel 23, hvor familien gis en videre positiv beskyttelse.) Praksis fra EMD viser likevel at bestemmelsen er blitt tolket slik at den til en viss grad gir statene en positiv plikt for tilrettelegging (som i saken Christine Goodwin mot Storbritannia av 11. juli 2002 (storkammer), avsnitt 72).

3.2 Eksempler på forhold som reguleres av menneskerettighetene

3.2.1 Om eksempelbruken

Nedenfor gjennomgås de ulike sentrale delene av privatlivsbestemmelsen, med utgangspunkt i avgjørelser fra EMD og kommentarer og synspunkter fra FNs menneskerettighetskomité (særlig UNHRC General Comment No. 16 1998 on the Right to Privacy). Denne saksgjennomgangen gir mer detaljering til de ulike elementene av artikkel 8 og SP artikkel 17. Men samtidig må det understrekes at nettopp innen EMK artikkel 8 har EMD vist at konvensjonen kan tolkes dynamisk, i takt med samfunnsutviklingen. Selv om det dynamiske elementet er fremtredende i kun et ytterst beskjedent antall saker, betyr det at det bildet som tegnes nedenfor, vil endres med tiden.

I tillegg må det legges vekt på at artikkel 8 er del av en større sammenheng. Artikkel 8 vil eksempelvis være den «nedre grense» til torturforbudet i EMK artikkel 3, og elementer vil gjenfinnes i religionsfrihetsbestemmelsen i EMK artikkel 9. Dersom artikkel 8 isoleres fra de øvrige bestemmelsene i konvensjonen, vil man kunne få en situasjon hvor man i norsk sammenheng kan tolke mer inn i denne bestemmelsen enn det man vil gjøre om den er del av et større hele (som EMK eller menneskerettsloven). I det følgende er det ikke tatt hensyn til en slik eventuell bredere inkludering av forhold som vil kunne omfattes av privatlivsreguleringen.

De sakene som presenteres nedenfor, er sortert alfabetisk ut fra tema. EMD har trukket frem forhold om både fysisk og psykisk integritet, som for så vidt har berøringspunkter med EMK artikkel 2 og 3. Videre er spørsmål om vern om ære og rykte blitt behandlet under artikkel 8, tilsvarende det som direkte nevnes avslutningsvis i SP artikkel 17(1) og som under EMK behandles i artikkel 10 om ytringsfrihet, men da som en begrunnelse for å gjøre inngrep i bestemmelsen. Saker om navn og identitet (derunder fotografier) er også blitt rubrisert under artikkel 8. Overvåkning og registre omfattes også, hvor det siste inkluderer både intime og fortrolige opplysninger, og offentlige og private registre. Andre aktuelle spørsmål som har funnet innpass, er forhold knyttet til personlig autonomi, seksualitet (særlig homofili), kjønnsskifte og helse. Abortspørsmål er behandlet under artikkel 8, dels som en forlengelse av helsespørsmål. Andre linjer kan trekkes til vern mot frihetsberøvelse (artikkel 5), tanke- og trosfrihet (artikkel 9), og forenings- og forsamlingsfrihet (artikkel 11).

En av årsakene til at vi har valgt å gjøre fremstillingen av forhold som reguleres av privatlivsbestemmelsen i EMK artikkel 8 relativt omfattende, er at det er viktig å få frem hvor mange rettsspørsmål som faktisk har en side til personvern/privatliv (uavhengig av den internrettslige rubriseringen). I norsk lovgivning, rettspraksis og teori er det bare i beskjeden grad tradisjon for å anse disse spørsmålene som spørsmål om personvern/privatliv. Vi håper således fremstillingen ikke bare tjener å få frem kompleksiteten og bredden i privatlivsbegrepet, men også får frem kontrasten til den internrettslige tilnærmingen til de rettslige spørsmålene; en tilnærming som innebærer at privatlivsaspektet ofte ikke kommer til sin rett. Dette vil igjen ha betydning for spørsmålet om vi bør grunnlovsfeste retten til personvern/privatliv, noe vi kommer tilbake til nedenfor i punkt 4.1.

I Personvernkommisjonens delutredning «Medier og personvern» (se punkt 1.3 ovenfor) gjennomgås en rekke saker fra EMD særlig innen forhold som vedrører behandling av personopplysninger. Disse sakene er tonet ned i fremstillingen nedenfor, og det henvises derfor til delutredningen for ytterligere detaljering. Tilsvarende er gjort i forhold til den omfattende redegjørelsen i Ytringsfrihetskommisjonen utredning (NOU 1999: 27 «Ytringsfrihed bør finde sted») vedrørende saker som berører ytringsfrihet og personvern/privatliv.

3.2.2 Abort

En kvinnes rett til abort reguleres i en menneskerettighetssammenheng ikke av retten til liv, men av privatlivsbestemmelsen i EMK artikkel 8. Forbud mot abort utgjør et inngrep i artikkel 8(1), og må derfor kunne rettferdiggjøres etter artikkel 8(2) for at ikke brudd skal konstateres. Det at menn ikke har avgjørelsesmyndighet i dette, er ikke noe inngrep etter artikkel 8(1), siden kvinnen er den personen som i hovedsak påvirkes av graviditet og abort (som i Boso mot Italia av 5. september 2002). En motsatt vinkling finnes i saken Evans mot Storbritannia av 10. april 2007 (storkammer), som aksepterte at en mann kunne kalle tilbake sitt samtykke til gjennomføring av kunstig befruktning.

Det er ikke mange abortsaker som er blitt behandlet av EMD. En sentral sak gjaldt informasjon om abortmuligheter, prevensjon og andre forhold om kvinners seksualitet (Open Door og Dublin Well Woman mot Irland av 29. oktober 1992). Disse to organisasjonene drev rådgivningsvirksomhet mellom annet om abortklinikker i England, en virksomhet irske myndigheter nedla forbud mot. EMD slo fast at dette forbudet krenket artikkel 10 om ytringsfrihet og rett til informasjon, og lot være å drøfte om dette også stred mot artikkel 8 og retten til privatliv.

3.2.3 Autonomi

Personlig autonomi reguleres av bestemmelsene om personvern/privatliv på ulike måter. Innen dette begrepet kan forhold som klær, språk, hår/skjegg, vennekrets, studier, helse, rusmidler, yrkesvalg, tradisjonsbundet levesett, tigging og mye annet omfattes. Mange saker fra EMD viser at mange stater her gjør inngrep i artikkel 8 uten at de har tilstrekkelig gode grunner.

Flere saker om rom-folket er behandlet av EMD (som for eksempel de fem sakene Chapman, Beard, Coster, Lee og Jane Smith mot Storbritannia, som alle ble behandlet av EMD i storkammer 18. januar 2001). Også saker om aktiv dødshjelp og selvvalgt avslutning av livet er blitt brakt inn for EMD (som Pretty mot Storbritannia av 29. april 2002), og selv saker om flytting av urner fra en urnelund til en annen er blitt diskutert (Elli Poluhas Dödsbo mot Sverige av 17. januar 2006).

Grensene for den personlige autonomien settes ikke bare av hensyn til samfunnet, men ofte også av hensyn til andres rettigheter og friheter.

3.2.4 Barn

Barns stilling kommer særlig frem i barnevernsaker som har vært ført for EMD. En sentral avgjørelse er Olsson mot Sverige av 24. mars 1988. Denne saken gjaldt tre svenske barn som midlertidig ble plassert i fosterhjem. Selve omsorgsovertakelsen var ikke i strid med EMK, ei heller at barna ble splittet, men EMD fant det konvensjonsstridig at de ble plassert i separate hjem så langt fra hverandre at samvær barna imellom og mellom barn og foreldre ble unødig vanskeliggjort. EMD ga uttrykk for at tiltaket ikke var gitt relevant og tilstrekkelig begrunnelse. Se her også R.K. og A.K. mot Storbritannia av 30. september 2008.

Det foreligger flere dommer mot de nordiske landene, særlig fordi inngrepene ikke alltid er i samsvar med loven, men også fordi de ikke alltid legger til rette for at foreldrene på sikt igjen kan bli forent med barna (se for eksempel Eriksson mot Sverige av 22. juni 1989). I Johansen mot Norge av 7. august 1996 ble fratakelse av foreldreansvar og nektelse av besøksrett funnet konvensjonsstridig etter artikkel 8, mens overtakelse av omsorg var akseptabelt. Saken K. og T. mot Finland av 12. juli 2001 gjaldt fjerning av barn umiddelbart etter fødselen. Barnevernssaker hører for øvrig ofte mer naturlig inn under EMK artikkel 6 om rettferdig rettergang enn under artikkel 8 om retten til familieliv.

Saken Hoffmann mot Østerrike av 23. juni 1993 gjaldt foreldreansvar etter skilsmisse. Her slo EMD fast at det å tilhøre trosretningen Jehovas Vitner ikke i seg selv kunne ekskludere noen fra foreldreansvar, og at det måtte en mer konkret vurdering til. Denne saken ble avgjort etter diskrimineringsbestemmelsen i EMK sammenholdt med privatlivsbestemmelsen (artikkel 14 jf. artikkel 8). Tilsvarende i Salgueiro da Silva Mouta mot Portugal av 21. desember 2001, hvor EMD fastslo at det forelå diskriminering siden myndighetene

hadde gitt moren foreldreretten i en barnefordelingssak alene fordi faren var homoseksuell (artikkel 14 sammenholdt med artikkel 8).

Litt i samme kategori er saken Keegan mot Irland av 26. mai 1994, som gjaldt adopsjon mot den biologiske farens vilje. Selv om moren og faren hadde skilt lag rett etter unnfangelsen, slo EMD fast at adopsjonen var et inngrep i hans familieliv. Inngrepet kunne ikke rettferdiggjøres etter artikkel 8 annet ledd, og det ble derfor konstatert brudd på EMK. En annen sak gjaldt adopsjon hvor barna protesterte, se Pini med flere mot Romania av 22. juni 2004.

Det tar ofte lang tid før nasjonale rettsmidler er uttømt i barnevernsaker, og enda lengre tid før prosessen for EMD er avsluttet. Konkluderer EMD med at nasjonale myndigheter har begått urett, for eksempel da barn og biologiske foreldre ble skilt, vil en tilbakeføring fort kunne resultere i at ny urett begås. Selv om det konstateres krenkelse, vil det dermed ikke være automatikk i at situasjonen på krenkelsestidspunktet gjenopprettes. EMD vil i denne sammenheng legge avgjørende vekt på hva som er det beste for barna (jf. for eksempel Bronda mot Italia av 9. juni 1998).

Praksis fra EMD er rik på saker som involverer barn. En rekke saker om farskap er avgjort, blant annet Shofman mot Russland av 24. november 2005. Disse sakene grenser opp mot artikkel 6 og rett til rettferdig rettergang. Motsatt vinkling finner vi i Jäggi mot Sveits av 13. juli 2006, hvor klageren fikk medhold i at det kunne tas prøver av en avdød person for å få avklart en tvist om farskap. I ytterkant av bestemmelsen finner en blant annet saker om sendrektig obduksjon av barn (Pannullo og Forte mot Frankrike av 30. oktober 2001).

Barn har for øvrig i utgangspunktet det samme vernet etter EMK artikkel 8 som det voksne har, men det vesentlige av praksis her knytter seg til foreldre som strides om behandlingen av barn. Barns rettigheter – også i forhold til personvern/privatliv – reguleres i tillegg av FNs barnekonvensjon, som er inntatt i menneskerettsloven av 1999.

3.2.5 Familieliv

Familiebegrepet er ikke helt sammenfallende for EMK og SP. EMK søker å finne frem til en alleuropeisk forståelse, mens SP i større grad overlater dette til hver enkelt stat. Det familiebegrepet som legges til grunn som utgangspunkt av EMD, omfatter i første rekke foreldre og barn. Dette gjelder barn uaktet deres status, og favner dermed adoptivbarn og barn født utenfor ekteskap. Dette følger både av ordlyden («no one» i SP artikkel 17 og «everyone» i EMK artikkel 8) og saken Marckx mot Belgia av 13. juni 1979, hvor EMD fant det konvensjonsstridig at Belgia hadde ulike arverettsregler for barn født i og utenfor ekteskap.

Formell status er ikke avgjørende, og således dekkes samboende foreldre på linje med gifte, noe som igjen åpner for konkrete vurderinger. Forholdet besteforeldre – barnebarn, foreldre – voksne barn og barn – barn kan også være familie etter en reell vurdering. Homoseksuelle er ikke vernet verken gjennom ordlyd eller praksis i forhold til familieliv, men mye av det samme vernet følger av privatliv (se 3.2.19 nedenfor). Det er også tale om familie selv om et par er frivillig eller ufrivillig barnløst. EMD har eksempelvis vurdert vilkår for ekteskapsinngåelse knyttet til slektsnærhet (B og L mot Storbritannia av 13. september 2005).

I én situasjon kan familien fremstå som en enhet overfor myndighetene, i en annen situasjon kan det være at familiemedlemmene står mot hverandre og myndighetene har en plikt til å beskytte en av partene. Det innebærer blant annet at også barna i en familie har en selvstendig rett til familieliv seg imellom. En annen innfallsvinkel er at barn kan ha familierelasjoner til mer enn én familie (som ved skilsmisse, omsorgsovertakelse og adopsjon) (se for eksempel Elsholz mot Tyskland av 13. juli 2000). Saker om trenering av samvær finnes det flere av, blant annet Hokkanen mot Finland av 23. september 1994.

Saken Johnston med flere mot Irland av 18. desember 1986 kan illustrere det at EMK ikke gir krav på skilsmisse. Johnston flyttet fra sin kone og sammen med en ny partner, og ønsket å skille seg fra den som på papiret var hans hustru. Det nye paret ble ikke hindret i faktisk å bo sammen, men Johnston ble nektet skilsmisse, og dermed fratatt muligheten til å gifte seg på nytt. Irland ble i denne saken dømt for brudd på artikkel 8 siden de ikke anerkjente det utenomekteskapelige barnet (faren var ikke «legal guardian» for datteren), men ikke for å ha nektet å innvilge formell skilsmisse. Se her også Kroon med flere mot Nederland av 27. oktober 1994, hvor EMD konstaterte krenkelse av artikkel 8 siden barnets rette far ikke kunne bli registrert som dette da moren var gift med en annen.

Saker om familieliv reguleres også av EMK artikkel 12 og EMK protokoll 7 artikkel 5, og FNs konvensjon om sivile og politiske rettigheter artikkel 23 og 24. Disse bestemmelsene regulerer

særlig retten til å inngå ekteskap og stifte familie, og likhet mellom ektefellene. Saken Petrovic mot Østerrike av 27. mars 1998 viser for øvrig at statene etter EMK ikke har noen plikt til å etablere ordninger for barselstønad.

Dersom et konkret saksforhold faller utenfor definisjonen av familieliv, vil forholdet ikke dekkes av artikkel 8(1), og det vil dermed ikke være noe inngrep i rettigheten. Og så lenge det ikke er noe inngrep i rettigheten, trenger myndighetene heller ikke rettferdiggjøre dette etter inngrepshjemmelen i artikkel 8(2). I slike tilfeller står myndighetene fritt i sin myndighetsutøvelse (i alle fall så lenge det ikke kommer i konflikt med andre rettigheter).

3.2.6 Forurensning

Saker om forurensning og vern om naturmiljø er også blitt vurdert under EMK artikkel 8. Dette kan gjelde ulike typer forurensning, som støy, støv, lukt og kjemikalier.

Saken Powell og Rayner mot Storbritannia av 21. februar 1990 gjaldt flystøy fra Heathrow. EMD fant at de negative følgene av flyplassen – særlig støy – rammet deres hjem på en måte som gjorde artikkel 8 anvendelig. I dette tilfellet forelå ingen krenkelse, siden forholdet etter EMDs skjønn falt innenfor Storbritannias skjønnsmargin. Da en lignende sak kom opp for EMD ti år etter, men nå begrenset til nattflyvning, fant EMD i første instans at myndighetene ikke hadde gjort nok for å begrense eller undersøke konsekvensene av den negative påvirkningen naboene ble utsatt for, men dette synet ble fraveket av EMD i storkammer (Hatton med flere mot Storbritannia av 7. august 2003). Begge disse sakene gjaldt rekkevidden av statens positive forpliktelser under artikkel 8. En nyere sak om støy er Moreno Gomez mot Spania av 16. november 2004. Denne saken gjaldt støy fra nattklubber, som holdt støynivå over det tillatte og heller ikke respekterte stengetider. EMD konstaterte at Spania her ikke hadde gjort tilstrekkelig for å bringe forholdet til opphør, og at det forelå krenkelse av EMK artikkel 8.

Saken López Ostra mot Spania av 9. desember 1994 gjaldt en annen type forurensning. Det var her tale om eventuelle positive forpliktelser som påhvilte spanske myndigheter, siden myndighetene etter klagerens syn ikke gjorde nok for å forhindre påvirkningen. López Ostra var nabo til et privat industriavfallsanlegg, som etter hennes oppfatning avga så mye lukt, lyd og forurensende gasser at hennes rett til respekt for hjem var krenket. EMD avveide hensyn til familien opp mot samfunnsmessige hensyn. Den la vekt på at myndighetene hadde tillatt byggingen av anlegget og ikke hadde iverksatt effektive tiltak mot den stadige forurensningen. På den annen side avhjalp anlegget et alvorlig byproblem og myndighetene hadde betalt López Ostras leie etter utflyttingen. Dette var likevel etter EMDs skjønn ikke nok til å imøtekomme den positive forpliktelsen som påhvilte myndighetene, og EMD konstaterte derfor krenkelse.

I en senere sak har EMD slått fast at myndighetene har en plikt til å informere om mulig forurensningsfare fra en nærliggende fabrikk, men denne gangen ble tilfellet vurdert under retten til respekt for privatliv (Guerra med flere mot Italia av 19. februar 1998). Se også helseaspektet drøftet i McGinley og Egan mot Storbritannia av 9. juni 1998 (omtalt nedenfor i underkapittel 3.2.18). En nyere dom mot Russland viser at staten kan pålegges ansvar for de helseskadene som oppstår når de tillater forurensning i kombinerte industri- og boligområder (Fadeyev mot Russland av 9. juni 2005).

3.2.7 Fotografier

Bruk av fotografier reguleres på ulike vis av vernet om personvern og privatliv (se også omtale under omdømme og overvåkning nedenfor). Slike forhold bringes gjerne inn for EMD med en annen vinkling, nemlig som begrensning av ytringsfriheten. Disse sakene vil i det vesentligste dreie rundt statens positive forpliktelser, det vil si pålegg om reguleringer i forholdet mellom private.

En sentral sak som kan illustrere dette, er von Hannover mot Tyskland av 24. juni 2004. Denne saken gjaldt prinsesse Carolines ønske om ikke å bli avbildet i ulike private situasjoner, som for eksempel under handleturer og kafebesøk (paparazzi-fotografering). EMD konkluderte med at hun hadde krav på beskyttelse ut fra vern om hennes privatliv, og indikerte samtidig en grense mellom offentlige personer og saker av offentlig interesse på den ene siden, og private forhold på den andre. Lignende saker har vært oppe for norske domstoler (som Big Brother-saken og Stenberg/Sætersaken).

En annen vinkling er publisering av fotografier i forbindelse med ettersøkning. I en sak som gjaldt gjennomføring av samvær ble slik publisering funnet å være i samsvar med EMK artikkel 8 (se A.B. mot Polen av 18. oktober 2001). Tilsvarende i en sak om fotografering og oppbevaring

av fotografiene i en straffesak (Murray mot Storbritannia av 28. oktober 1994)

Se mer om reguleringen av fotografier i Ytringsfrihetskommisjonen utredning (NOU 1999: 27 «Ytringsfrihed bør finde sted»), Personvernkommisjonens delrapport, og den omfattende gjennomgangen i Borvik: Personvern og ytringsfridom (2008).

3.2.8 Frihetsberøvelse

Frihetsberøvelse i seg selv reguleres i hovedsak av EMK artikkel 5. Her finnes detaljerte regler i selve konvensjonen, og mange presiseringer er gjort av EMD i et stort antall saker. Utgangspunktet er at frihetsberøvelse vil være et inngrep også i retten til privatliv, men at inngrepet kan rettferdiggjøres gjennom de forholdene som oppstilles i artikkel 5. Frihetsberøvelsen kan grunnes i ulike tilfeller som soning, varetekt, politiarrest, barnevern, smittespredning, utsending av utlendinger og medisinsk behandling.

En annen tilnærming er at i slike situasjoner med frihetsberøvelse, vil individene fortsatt ha krav på at deres rettigheter etter EMK artikkel 8 respekteres i den grad det er mulig (jf. Boyle og Rice mot Storbritannia av 27. april 1988). Selv om familielivet klart nok reduseres gjennom frihetsberøvelse, vil for eksempel spørsmål om besøk kunne bli regulert av retten til respekt for sitt privatliv (se Ostrovar mot Moldova av 13. september 2005). Tilsvarende vil retten til korrespondanse bli beskåret (blant annet av sikkerhetsgrunner), men myndighetene skal ikke gjøre inngrep i rettigheten i større grad enn hva som kreves av situasjonen (se her også punkt 3.2.14 om korrespondanse nedenfor). I forhold til barn, vil for eksempel det ikke være akseptabelt at fengselsstraff automatisk fører til at den fengslede fratas foreldremyndighet (jf. Sabou og Pircalab mot Romania av 28. september 2004).

3.2.9 Hjem

Hjem nevnes eksplisitt i EMK artikkel 8. Der det forekommer inngrep, vil dette i mange tilfeller være relativt lett å rettferdiggjøre for myndighetene. Presisering av begrepet hjem er vanskeligere.

FNs menneskerettighetskomité har gitt en kort bemerkning knyttet til SP artikkel 17, hvor en vid tilnærming legges til grunn (UNHRC General Comment No. 19 1990 avsnitt 5): «The term ‹home› in English, ‹manzel› in Arabic, ‹zhùzhái› in Chinese, ‹domicile› in French, ‹zhilische› in Russian and ‹domicilio› in Spanish, as used in article 17 of the Covenant, is to be understood to indicate the place where a person resides or carries out his usual occupation.» EMD støtter denne vide forståelsen, og har i tillegg slått fast at også kontorlokaler kan omfattes (Chappell mot Storbritannia av 30. mars 1989). Her ble det foretatt undersøkelse i eiendom som var både bolig og forretning, selv om formålet med undersøkelsen kun var forretningsdelen (se også nedenfor punkt 3.2.17). EMD kom frem til at dette var dekket av begrepet hjem, og dermed inngrep i artikkel 8(1). Noen krenkelse forelå ikke siden inngrepet var rettferdiggjort etter annet ledd. Slike tilfeller glir ofte bort fra hjem og over i privatliv. I andre saker har EMD slått fast at campingvogner og bobiler kvalifiserer til hjem, dersom den faktiske bruken tilsier det. Se også grensedragningen i Halford mot Storbritannia av 25. juni 1997.

EMK artikkel 8 gir ikke krav på et hjem, det er tale om respekt for det hjemmet en har. En sak om å kaste ut leietakere førte derfor ikke frem under artikkel 8, se Velosa Barreto mot Portugal av 21. november 1995. To private grupper ble her satt opp mot hverandre, hvor leietakerne vant frem. Domstolen la vekt på at reguleringen ikke var vilkårlig og at det var god balanse mellom gruppene. EMD vil samtidig være på vakt mot forhold som leder til at EMD indirekte må ta stilling til økonomiske, sosiale og kulturelle rettigheter under EMK.

EMD har drøftet mange ulike tilfeller under denne overskriften. I saken Gillow mot Storbritannia av 24. november 1986 hadde et ektepar kjøpt et hus som de siden leide ut møblert i en lang periode. Da de skulle flytte tilbake, fikk de ikke bosettingstillatelse fordi de ikke hadde «residence qualifications», slik det krevdes etter nye regler som skulle sikre fast bosetting for lokalbefolkningen. Huset sto tomt, det fantes ingen potensielle leietakere, og Gillows hadde intet annet sted å bo. EMD slo fast at dette utgjorde et inngrep i deres rett til respekt for hjem, og at det ikke forelå proporsjonalitet mellom tiltak og mål i denne konkrete saken. EMK var dermed krenket.

Statsklagesaken Kypros mot Tyrkia av 10. mai 2001 gjaldt også retten til hjem, hvor EMD konkluderte med at Tyrkias mange og ulike tiltak vanskeliggjorde realiseringen av rettigheten på en måte som resulterte i krenkelse av artikkel 8.

Flere av sakene knyttet til hjem dreier seg om offentlige reguleringer i form av planarbeid eller sosiale og økonomiske tiltak. I slike saker vil statene tilstås en vid skjønnsmargin av EMD. Mot-

satt tilnærming tas der staten ikke følger egne oppstilte prosedyrekrav (som i Buckley mot Storbritannia av 25. september 1996), siden man her beveger seg over mot spørsmål om rettssikkerhet, som er i kjernen av EMKs virkefelt.

3.2.10 Husundersøkelser

Husundersøkelser er et sentralt område under EMK artikkel 8. Her vil det like gjerne være tale om inngrep i privatliv og korrespondanse som hjem. Eksempler fra EMDs praksis bidrar til å klargjøre innholdet (se her også Personvernkommisjonens delrapport «Medier og personvern» og punktene 3.2.9 og 3.2.17).

I saken Funke mot Frankrike av 25. februar 1993 slo EMD fast at alle rettighetene i artikkel 8(1), med unntak for familieliv, var aktuelle. Denne saken gjaldt husundersøkelser foretatt av franske tollmyndigheter i forbindelse med en valutasak. EMD vurderte lovgrunnlag og det anførte formålet før den diskuterte om inngrepet var nødvendig i et demokratisk samfunn. Domstolen viste til at økonomisk kriminalitet var kompleks og måtte kunne møtes med et bredt spekter av virkemidler, men at «the relevant legislation and practice must afford adequate and effective safeguards against abuse» (dommens avsnitt 56). EMD mente at slike mekanismer ikke fantes i dette tilfellet, og at bestemmelsen dermed var krenket. Se her også Societes Colas Est med flere mot Frankrike av 16. april 2002, som også viser at artikkel 8 er relevant i saker knyttet til næringsliv (i dette tilfelle konkurranserett).

Saken Niemietz mot Tyskland av 16. desember 1992 kan også tjene som eksempel. Her hadde tyske myndigheter gjennomført undersøkelser i kontorene til en advokat for å finne frem til en persons rette identitet. Domstolen slo fast at dette var et inngrep i privatliv og hjem, selv om det var tale om et næringsforhold. Tiltaket hadde klart nok hjemmel i lov, og det søkte å nå ett av de oppstilte formålene i artikkel 8(2). Igjen var det springende punktet om tiltaket var nødvendig i et demokratisk samfunn. EMD konsentrerte drøftelsen til om hvorvidt det forelå proporsjonalitet mellom mål og middel, men fant at så ikke var tilfelle, og at EMK dermed var krenket. I saken Ernst med flere mot Belgia av 15. juli 2003 ble det konstatert krenkelse i en husundersøkelse rettet mot journalister, denne gangen fordi hjemmelsgrunnlaget var svakt.

3.2.11 Innvandring

Innvandring som tema faller utenfor privatlivsbestemmelsen, men innvandreres familieliv reiser mange spørsmål – både i forhold til innreise og tvungen utreise (utvisning) – som vil kunne omfattes av bestemmelsen. Dette er et politisk sensitivt område, og EMD gir statene et rommelig skjønn. Når det gjelder innreise, finnes det ikke noe ubetinget menneskerettslig krav på innreise til et annet land (men sammenlign her med FNs verdenserklæring om menneskerettigheter av 1948). Praksis fra EMD er særdeles omfattende på dette feltet.

Det som ofte blir en menneskerettslig problemstilling, er om innvandrere som allerede har opphold i landet, har krav på å få brakt sin familie over til dette nye landet. Saken Abdulaziz, Cabales og Balkandali mot Storbritannia av 28. mai 1985 er illustrerende. Denne saken gjaldt en kvinne som ble nektet gjenforening i England med sin tyrkiske mann. Begrunnelsen var at hun ikke var engelsk statsborger av fødsel. Loven gjorde det samtidig vanskeligere for kvinner å gjenforenes med sine menn enn omvendt. EMD slo fast at artikkel 8 var berørt, selv om fjerde tilleggsprotokoll til EMK hadde spesialregler om dette. Videre slo den fast at «familie» også kan dekke planlagt familie. Vilkåret var at partene selv oppfattet seg som gifte par, som enten hadde bodd sammen eller ønsket å bo sammen. EMD kom likevel frem til at den positive forpliktelsen ikke strakk seg så langt som dette tilfellet krevde. Den la vekt på at myndighetene ikke hadde noen generell plikt til å akseptere individenes valg av bostedsland, at paret like gjerne kunne bo i Tyrkia som i England, og at klagerne kjente til problemene med innreise da de giftet seg. Derimot konkluderte EMD med at artikkel 14 jf. artikkel 8 var brutt i forhold til kjønnsdiskriminering.

Skilsmisse kan i mange tilfeller lede til utvisning av en utlending, men gjennom barnet kan foreldrene få rett til opphold. Slik sett fører oppløsningen av parforholdet til at det oppstår to selvstendige «familier». Berrehab mot Nederland av 18. februar 1988 kan tjene som illustrasjon. Berrehab ble skilt fra sin nederlandske kone, som han hadde ett barn med. Den fraskilte hustruen hadde omsorgen for barnet, men Berrehab så datteren fire ganger i uken og flere timer hver gang. Hans oppholdstillatelse ble ikke forlenget på grunn av skilsmissen, og han ble utvist fra Nederland siden han ikke hadde slik oppholdstillatelse. EMD slo fast at det fortsatt forelå familiebånd til datteren,

og at det ikke kunne kreves at moren flyttet med ham til Marokko. Inngrepet var ikke rettferdiggjort etter annet ledd, selv om myndighetene gis en vid skjønnsmargin når det gjelder innvandring. Se for eksempel også Mehemi mot Frankrike av 26. september 1997.

Kriminalitet kan også lede til utvisning, noe som kan illustreres av saken Moustaquim mot Belgia av 13. juli 1991. Moustaquim hadde en lang serie kriminelle forhold bak seg, og det var stor risiko for tilbakefall. Dette var ikke tilstrekkelig alvorlig til at tiltaket ble funnet proporsjonalt: Han hadde langt opphold i Belgia (20 år), familien bodde der, han hadde bare bodd i Marokko frem til han var år, hele hans utdannelse var i fransk, og kriminaliteten var begått som ungdom. Selv om kriminalitetens alvor ofte er avgjørende for rettsfølelsen, vil EMD legge stor vekt på oppholdstid i deportasjonsland og oppholdsland, bånd til begge land og konsekvenser av utvisning. I disse sakene gir EMD relativt stort spillerom til statene. Nasri mot Frankrike av 13. juli 1995 og Boultif mot Sveits av 2. august 2001 bekrefter den vide skjønnsmarginen her. I slike tilfeller vil det ikke være tale om dobbeltstraff i juridisk forstand, selv om utvisningen i slike tilfeller ofte vil bli oppfattet som den reelle sanksjonen sett fra den utvistes side (jf. Üner mot Nederland av 18. oktober 2006).

3.2.12 Integritet

Et av kjerneområdene for EMK artikkel 8 er fysisk og psykisk integritet. EMD har her i stor grad pålagt myndighetene positive forpliktelser. Det vil si at det ikke er tilstrekkelig at myndighetene selv unnlater å gjøre inngrep, men at de også må treffe konkrete tiltak for å sikre at rettighetene realiseres.

En sentral dom er X og Y mot Nederland av 26. mars 1985. Denne saken gjaldt en funksjonshemmet jente som hadde blitt voldtatt av pleiepersonell ved en privat institusjon. Hun kunne etter nederlandsk rett ikke anlegge sak selv, samtidig som faren (vergen) heller ikke hadde slik myndighet. Dette hullet i loven ble nederlandske myndigheter funnet ansvarlige for. EMD slo fast at det forelå inngrep i artikkel 8(1), og at unntaket ikke kunne bli rettferdiggjort etter artikkel 8(2). Dommen viser at artikkel 8 til en viss grad krever at staten treffer positive tiltak for å regulere forhold mellom individene. Vern om fysisk integritet i psykiatrisk institusjon var oppe i Storck mot Tyskland av 16. juni 2005. Jf. også Stubbings med flere mot Storbritannia av 22. oktober 1996, om tilrettelleggelse av rettsprosess ift. erstatning i tilfelle av seksuelle overgrep.

Costello-Roberts mot Storbritannia av 25. mars 1993 er en annen sentral sak. Forholdet her var at rektor ved skolen hadde slått en elev tre ganger på baken med gymsko. Domstolen uttalte at tiltak innen skoleverket kan berøre retten til respekt for privatlivet, men at ikke alle tiltak som berører den fysiske eller psykiske integriteten kan sies å være et inngrep i artikkel 8. Siden dette falt utenfor artikkel 8, var det heller ikke nødvendig for EMD å gå inn på EMK artikkel 3 om nedverdigende eller umenneskelig behandling eller straff.

Medisinske eksperimenter uten samtykke vil være inngrep etter artikkel 8(1), men saker om dette hører mer naturlig hjemme under artikkel 3. Her kan også artiklene 5 og 6 om frihetsberøvelse og rett til rettferdig rettergang være aktuelle. Tilsvarende for mer generelle medisinske undersøkelser og tiltak, som vaksinasjonsprogrammer eller helseundersøkelser. Men se Glass mot Storbritannia av 9. mars 2004 som behandler dette under artikkel 8. Jf. også Trocellier mot Frankrike av 5. oktober 2006, som gjaldt erstatning i etterkant av feilbehandling ved sykehus (krenkelse), og Pentiacova med flere mot Moldova av 4. januar 2001, som gjaldt tilgang på kostbar medisinsk behandling (ikke krenkelse).

Kroppsvisitering kan også behandles etter EMK artikkel 3. Prøvetaking (blod, urin, hår) for DNA-testing, for eksempel i forbindelse med kriminalsaker, kan lett komme i konflikt med ens integritet. Se her for eksempel Murray mot Storbritannia av 28. oktober 1994 om DNA-prøvetaking og oppbevaring av informasjon i et register i forbindelse med straffesak, eller Mikulic mot Kroatia av 7. februar 2002, som gjaldt tvungen DNA-prøve i forbindelse med farskap (krenkelse på grunn av svak lovhjemmel). På samme måte behandles psykiatriske undersøkelser. Selv fotografier og fingeravtrykk kan ses som inngrep i retten til privatliv. Også saker mellom private kan omfattes, som i Madsen mot Danmark av 7. november 2002, en sak som gjaldt urinprøver på en privat arbeidsplass.

En stor debatt i Norge og andre land er rekkevidden av statens forpliktelse til å hindre vold i nære relasjoner, synliggjort blant annet gjennom Amnesty Internationals arbeid. Her er en inne i eventuelle positive forpliktelser staten pålegges gjennom EMK artikkel 8 og SP artikkel 17. Skjønnsmarginen for staten er her vid, og EMD vil vurdere konkret de ulike tiltakene statene har iverksatt for å hindre overgrep, men vil samtidig

være tilbakeholden med å overprøve disse. I saken M.C. mot Bulgaria av 4. desember 2003 fant EMD at staten ikke hadde gjort nok for å beskytte mot seksuelle overgrep.

Dersom det foreligger inngrep i rettigheten, må inngrepet kunne rettferdiggjøres etter bestemmelsens annet ledd for at staten skal kunne gå fri. Selv om integritetsinngrep befinner seg i kjerneområdet av artikkel 8, vil statens myndigheter ha relativt vide muligheter for å kunne forsvare inngrep i privatlivet også i disse tilfellene.

3.2.13 Kjønnsskifte

EMD har tatt stilling til spørsmål omkring kjønnsskifte i en rekke saker, som i Rees mot Storbritannia av 17. oktober 1986 og Christine Goodwin mot Storbritannia av 11. juli 2002 (storkammer). EMD har vært forsiktig med å vise vei når det ikke finnes noen enhetlig europeisk standard. Men domstolen har vært villig til å strekke konvensjonens ordlyd så langt i tilfeller om kjønnsskifte (når den har kommet frem til en rettsenhet er under utvikling) at det nok er riktigere å omtale dette som rettsutvikling heller enn rettsanvendelse.

Reguleringen av kjønnsskifte trekker også linjer til praksis knyttet til homofili (og i menneskerettslig litteratur gjerne behandlet som LGBT – lesbian, gay, bisexual and transgender persons), se mer i underpunktet 3.2.19 nedenfor.

3.2.14 Korrespondanse

Korrespondanse er eksplisitt opplistet i EMK artikkel 8. Korrespondanse glir fort over i de andre elementene i bestemmelsen, særlig privatliv. Korrespondanse må ses vidt, særlig sammenholdt med de andre elementene i første ledd. Selv om ordlyden opprinnelig siktet inn mot brev og post, vil en i dag inkludere telefon, telefaks, mobiltelefon, internett, epost og privatradioer. Se her også Personvernkommisjonens delrapport «Medier og personvern».

EMD har behandlet mange saker om korrespondansen til innsatte i fengsler. De tidligste sakene søkte å etablere en form for «innebygget begrensning» i rettighetene, i den forstand at noen mennesker – som innsatte i fengsler eller vernepliktige – var i en slik situasjon at rettigheten ikke var anvendelig. I disse tilfellene skulle det derfor ikke være nødvendig å begrunne tiltaket etter inngrepshjemmelen. Denne praksisen ble fraveket i saken Golder mot Storbritannia av 21. februar 1975. Saken gjaldt en innsatt i et fengsel som urikktig hadde blitt knyttet til et fangeopprør. Han skrev brev om dette til en advokat, men fengselsledelsen holdt brevene tilbake fordi han ikke først hadde søkt å ordne opp internt. EMD slo fast at dette var et inngrep i Golders rett til respekt for sin korrespondanse. Inngrepet var ikke nødvendig for å nå de oppstilte formålene i annet ledd, og EMD konstaterte at Storbritannia krenket EMK. I flere senere praksis har EMD slått fast at det skal mye til før inngrep i innsattes korrespondanse kan godtas.

Silver med flere mot Storbritannia av 25. mars 1983 er en annen sentral sak. Denne saken gjaldt fanger i et britisk fengsel, hvor de opplevde at fengselsmyndighetene sensurerte innkomne og utgående brev, mellom annet til familie og advokat om fengselsforhold, rettssaker og forretninger. Det fantes mange aktuelle direktiver om postkontroll, men noen av disse var unntatt offentlighet. EMD kom først til at det forelå brudd på EMK artikkel 6(1) siden en klage om tilsvarende forhold hadde blitt avvist uten realitetsbehandling av innenriksministeren. Deretter slo den fast at det forelå inngrep i artikkel 8(1). Inngrepshjemmelen ble vurdert, hvor EMD først kom frem til at inngrepet var i samsvar med loven: det var tilstrekkelig at det forelå grunnlag i engelsk rett. Lovskravet var derimot ikke oppfylt når det kom til de hemmeligholdte reglene: dette stred mot kravet om forutsigbarhet. De øvrige brevene ble vurdert helt konkret i forhold til kravet om at tiltaket skal være nødvendig i et demokratisk samfunn, hvor inngrepene måtte være begrunnet i et presserende sosialt behov og det måtte foreligge forholdsmessighet mellom mål og middel. Etter EMDs skjønn måtte dette tolkes snevert, og settes opp mot de innsattes hensyn (for eksempel i forhold til rehabilitering). EMD kom etter denne konkrete vurderingen frem til krenkelse av EMK artikkel 8 for ytterligere seks brev.

Korrespondanse med advokat ble drøftet også i Campbell mot Storbritannia av 25. mars 1992. Campbell var innsatt på livstid, og klaget over at hans korrespondanse med advokaten ble åpnet og lest av fengselspersonell. EMD slo fast at dette var et inngrep i korrespondansen, og vurderte deretter om vilkårene for inngrep var til stede. Den slo fast at mulighetene for misbruk var svært store, både fra myndigheter og innsatte, og at det derfor stilles strenge krav til prosedyrer. Utgangspunktet er at brev bare kan åpnes hvis det foreligger konkret mistanke, og at den innsatte i så fall skal være til stede under åpningen. Bare i eksepsjonelle tilfeller kan myndighetene lese brevene.

EMD konkluderte med at det ikke forelå tilstrekkelige grunner for å gjøre inngrep, og at EMK artikkel 8 dermed var krenket. Viktig i denne sammenheng er også Schönenberger og Durmaz mot Sveits av 20. juni 1988.

EMD har også vurdert saker der frihetsberøvelsen ikke skyldes kriminelle forhold, men medisinske (som i Herczegfalvy mot Østerrike av 24. september 1992). Tilsvarende har EMD behandlet saker knyttet til økonomiske forhold, som i Foxley mot Storbritannia av 20. juni 2000 (innsyn i korrespondanse i forbindelse med konkurs).

3.2.15 Navn

EMK artikkel 8 regulerer også navn (knyttet til identitet). I saken Burghartz mot Sveits av 22. februar 1994 ble en mann nektet å beholde sitt gamle etternavn som mellomnavn etter at han hadde tatt sin hustrus etternavn ved giftemål. Etter sveitsisk lov hadde derimot kvinner en slik rett. Flertallet i EMD vurderte dette som brudd på artikkel 14 sammenholdt med artikkel 8, det vil si kjønnsdiskriminering som ikke ble rettferdiggjort. Siden artikkel 14 ikke er selvstendig, men fordrer at forholdet faller inn under en av konvensjonens øvrige bestemmelser, ble navn dermed indirekte vernet. EMD uttalte at navn er personlig identifikasjon og gir tilknytning til familie, og at samfunnet står relativt fritt i forhold til å regulere bruk av navn. Det må tas hensyn til at navn knytter bånd til andre mennesker, både i forretningssammenheng og privat.

I en senere sak (Stjerna mot Finland av 25. november 1994) slo EMD fast at navn ikke direkte nevnes i artikkel 8, men er et middel til personlig identifikasjon og bånd til familie, og derfor har betydning både for privatliv og familieliv. En persons frihet til å endre navn er ikke like opplagt et inngrep i 8(1) som plikten til å endre navn, men det påligger offentlige myndigheter en plikt til positive tiltak for at vern om privatliv skal være effektiv. Offentlig interesse i å regulere navnebruk hindret ikke at dette derfor var et inngrep i artikkel 8(1). EMD uttalte videre at staten har en vid skjønnsmargin med hensyn til regler som forandrer navn, særlig fordi det på dette feltet ikke foreligger særlig grad av rettsenhet i Europa. Domstolen vurderer i denne saken kun omfanget av den positive forpliktelsen og dermed rekkevidden av artikkel 8(1), og går ikke inn på artikkel 8(2).

3.2.16 Omdømme og ære

Omdømme og ære omfattes av EMK artikkel 8. Utgangspunktet vil her være en avveining av interesser som vernes gjennom EMK artikkel 8 om privatliv på den ene siden og EMK artikkel 10 om ytringsfrihet på den andre siden. Saker om dette drøftes ofte med utgangspunkt i ytringsfrihetsbestemmelsene. Myndighetene vil ikke kunne gjøre inngrep i ytringsfriheten ut over det som følger av ytringsfrihetsbestemmelsene, og således vil disse bestemmelsene sette rammer for hva som kan kreves i medhold av privatlivsbestemmelsene.

Fra EMD og FNs menneskerettighetskomité foreligger det rikholdig praksis. Prinsipielt viktige dommer er for eksempel Lingens mot Østerrike av 8. juli 1986 og Radio France med flere mot Frankrike av 30. mars 2004, som begge omhandler politiske forhold. Se her også Gourguenidze mot Georgia av 17. oktober 2006, som gjaldt beskyldninger om tyveri fremsatt i en avis hvor klager var avbildet og nevnt ved navn. Klager fikk ikke medhold i sitt injuriesøksmål for nasjonale domstoler, og EMD konkluderte med at hans rett til respekt for sitt privatliv ikke i tilstrekkelig grad var vernet. Flere norske saker er avgjort av EMD, for eksempel Bladet Tromsø og Stensaas mot Norge av 20. mai 1999 (selfangst), Bergens Tidende med flere mot Norge av 2. mai 2000 (plastisk kirurgi) og Tønsbergs Blad AS og Haukom mot Norge av 1. mars 2007 (boplikt).

Det vises her til den omfattende redegjørelsen i Ytringsfrihetskommisjonen utredning (NOU 1999: 27 «Ytringsfrihed bør finde sted») og Borvik: «Personvern og ytringsfridom» (2008), og dels også til Personvernkommisjonens delrapport om «Medier og personvern».

3.2.17 Overvåkning

Overvåkning av enkeltpersoner, for eksempel fra sikkerhetspoliti, kan lede til inngrep i alle de fire tilfellene som oppstilles i EMK artikkel 8(1). Oftest er det tale om inngrep i privatlivet, gjerne kombinert med korrespondanse. Personvernkommisjonens delrapport «Medier og personvern» gjennomgår noen sentrale saker om dette, og praksis fra EMD er på dette området svært omfattende (jf. også ovenfor punkt 3.2.9).

Saken Klass med flere mot Tyskland av 6. september 1978 er en prinsipielt viktig sak. Her var det tale om overvåkning av enkeltindividers post og telefon. EMD måtte først avklare om partene var ofre eller ikke, siden tyske myndigheter ikke

ville gi uttrykk for om de var blitt overvåket eller ei. Domstolen slo fast at måten det tyske systemet var organisert på, ledet til mulig inngrep i rettighetene til alle relevante personer. Det var klart nok at avlytting av telefonsamtaler var inngrep i retten til privatliv og korrespondanse. EMD slo fast at det forelå lovhjemmel og relevant formål, og testen sto her som så ofte ellers om inngrepet i rettigheten var nødvendig i et demokratisk samfunn. Her gikk EMD inn i en konkret vurdering av hvilke adekvate og effektive garantier det var oppstilt for å hindre misbruk av overvåkningshjemmelen, satt opp mot den trusselen terrorvirksomhet og spionasje utgjorde for et demokrati. Selv om det ikke fantes rene rettslige mekanismer, var det tilstrekkelig med de administrative og parlamentariske kontrollmekanismene som var etablert.

Telefonavlytning var tema også i Malone mot Storbritannia av 2. august 1984. I forbindelse med en helerisak hadde telefonen hans blitt avlyttet, samtidig som myndighetene hadde registrert og analysert den tekniske samtaleinformasjonen (om hvilke telefonnumre som er ringt når og hvor lenge). EMD slo fast at begge deler var inngrep i hans korrespondanse. Det var ikke avgjørende at han i kontrakten med selskapet hadde godtatt at teknisk informasjon ble registrert, poenget her var at teleselskapet ikke hadde rett til å gi dette videre til myndighetene. Inngrepet kunne ha vært godtatt etter annet ledd, men siden loven var upresis og lite tilgjengelig, konstaterte EMD at det forelå brudd på konvensjonen. Se her også Amann mot Sveits av 16. februar 2000.

Saken Lüdi mot Sveits av 15. juni 1992 gjaldt en narkotikalanger som tilbød en hemmelig politiagent å kjøpe kokain. Myndighetenes bruk av telefonavlytting var et inngrep etter artikkel 8(1), men dette var etter EMDs skjønn rettferdiggjort etter 8(2). Bruken av hemmelig politiagent ble ikke sett på som inngrep etter artikkel 8(1) fordi langeren måtte godta en innebygget begrensning i artikkel 8(1) siden hemmelige agenter var kjent som et tiltak mot den typen alvorlig kriminalitet han hadde involvert seg i, og det forelå dermed heller ikke her krenkelse. I Valenzuela Contreras mot Spania av 30. juli 1998 oppstiller EMD de rettssikkerhetskravene domstolen mener er nødvendige for akseptabel telefonavlytning som tiltak i straffesaker.

En annen vinkling finner vi i saken Peck mot Storbritannia av 28. januar 2003. Overvåkningskameraer fanget opp Peck mens han nattestid vandret rundt med en kniv, og bildene ble distribuert som eksempel på nytteverdien av slik overvåkning i forhold til kriminalitetsbekjempelse. Det viste seg imidlertid at Peck ikke var kriminell, men vurderte selvmord. EMD slo fast at dette krenket Pecks rett til respekt for sitt privatliv, selv om han beveget seg i det offentlige rom. Saken Perry mot Storbritannia av 17. juli 2003 behandler også avledet bruk av overvåkningskamera, denne gangen i forbindelse med vitneutpeking.

3.2.18 Personregistre

Politiregistre med nøytrale opplysninger (som navn, adresse, telefon etc.) var opprinnelig ikke regnet som inngrep i artikkel 8(1). I dag er holdningen en annen, blant annet på grunn av samfunnsutviklingen med økende antall registre og muligheter for samkjøring av opplysninger. En lang rekke saker om registre har vært oppe for EMD (se her også gjennomgangen i Personvernkommisjonens delrapport). De fleste sakene knytter seg til den registrertes rett til innsyn i registrene, men noen saker tar også opp legitimiteten av å opprette og føre registre. Her skal vi se på det første, mens det sistnevnte hører bedre inn under overvåkning.

Saken McGinley og Egan mot Storbritannia 9. juni 1998 gjaldt tjenestemenn som hadde deltatt i myndighetenes eksperimentering med atomvåpen ved Christmas Island. Tjenestemennene mente de hadde blitt utsatt for stråling som kunne ha ledet til senere skader og sykdom. De hevdet at informasjon myndighetene hadde både om dem og saken kunne bidra til at de fikk økt krigspensjon, men myndighetene ville ikke frigi informasjonen. EMD kom frem til at dette var et inngrep i artikkel 8(1), men siden klagerne ikke hadde utnyttet en administrativ klageordning, var ikke bestemmelsen krenket.

Saken Gaskin mot Storbritannia av 7. juli 1989 illustrerer en litt annen type problemstilling. Denne saken gjaldt registrering av opplysninger knyttet til barnevern (blant annet opphold på private barnevernsinstitusjoner) som Gaskin krevde innsyn i. EMD konstaterte inngrep i artikkel 8(1) fordi dette gjaldt opplysninger om svært personlige sider ved oppvekst, utvikling og historie. EMD slo fast at det er en positiv plikt for myndighetene til å tilrettelegge for innsyn i slike registre. I denne saken var det ubalanse mellom statens behov for hemmelighold av hensyn til kildevern og nøytralitet, og Gaskins behov for å bli bedre kjent med sin egen historie. Det spilte inn at det var en absolutt regel hvor statens hensyn gikk foran. Argumente-

ne gjelder generelt: Staten har plikt til å tilrettelegge gjennom lover, informasjon og andre praktiske tiltak også for private registre. Tilsvarende resultat kom EMD i M.G. mot Storbritannia av 24. september 2002. En lignende sak finner vi i Odièvre mot Frankrike av 13. februar 2003, som ble avgjort av EMD i storkammer. Her ønsket klageren innsyn i morens identitet mot hennes vilje, noe EMD konstaterte at klageren ikke hadde krav på.

En annen sentral dom knyttet til samme problemstilling som over, er Z mot Finland av 25. februar 1997. Denne saken gjaldt en finsk HIV-smittet dame som hadde vært gift med en HIV-smittet mann. I forbindelse med en straffesak mot mannen, om spredning av nettopp HIV-smitte, ble svært personlige forhold om hennes medisinske bakgrunn belyst i retten. Blant annet ble hennes leger ført som vitner og legejournalene lagt frem som bevis. EMD kom frem til at dette inngrepet i hennes privatliv kunne forsvares, men fastslo at hennes rettigheter var krenket i forhold til at identitet ikke ble holdt hemmelig lengre enn ti år. Saken M. S. mot Sverige av 27. august 1997 omhandler lignende forhold. Denne saken gjaldt medisinsk informasjon (blant annet om en gjennomført abort) et sykehus hadde gitt et forsikringsselskap i forbindelse med en prosess om erstatning. EMD slo fast at overlevering av slik personlig informasjon var et inngrep i retten til respekt for privat- og familieliv, men at vilkårene for rettmessig inngrep etter artikkel 8(2) var til stede. Se her også L.L. mot Frankrike av 10. oktober 2006, som gjaldt urettmessig fremleggelse av legejournaler i en skilsmissesak.

Leander mot Sverige av 26. mars 1987 er også relevant, og belyser en annen type situasjon. Denne saken omhandler både legitimiteten av overvåking og nektelse av innsyn. Leander hevdet at informasjon fra et hemmelig politiregister hindret ham fra å få permanent jobb ved det militæranlegget der han var midlertidig ansatt, og videre også førte til at han ble oppsagt fra sin midlertidige stilling. Dette, sammen med at han ikke selv fikk tilgang til denne informasjonen, mente han krenket hans rettigheter etter artikkel 8. EMD slo fast at innhenting og oppbevaring av informasjon, frigivelse av disse til andre myndigheter og nektelse av innsyn alle var inngrep etter art 8(1) – uansett hva registeret måtte inneholde. Denne saken var etter EMDs syn spesiell på grunn av statens behov for hemmelighold, og EMD kom til at inngrepet var rettferdiggjort etter 8(2). EMD konstaterte at statene har en vid skjønnsmargin når det gjaldt beskyttelse av nasjonal sikkerhet, noe som beskjærer EMDs mulighet til å overprøve myndighetenes vurdering. Utfallet var det motsatte i for eksempel Antunes Rocha mot Portugal av 31. mai 2005.

3.2.19 Seksualitet

Seksuelle forhold er i den indre kjernen av retten til respekt for privatliv, og har blitt behandlet av EMD i ulike saker (som Bensaid mot Storbritannia av 6. februar 2001). Flere av disse sakene har knyttet seg til kjønnsskifte, seksuell minstealder, abort, prevensjon, prostitusjon og homoseksualitet. De første sakene som ble behandlet under EMK avviste at slike forhold – særlig om kjønnsskifte og homofili – var dekket av artikkel 8, men EMD har gradvis endret tilnærming her.

I saken Dudgeon mot Storbritannia av 22. oktober 1981 slo EMD fast at et forbud mot homofili utgjorde et inngrep i artikkel 8(1). I dette tilfellet var inngrepet rettferdiggjort med hensyn til seksuell minstealder for homofile på 21 år i stedet for 18 år for heterofile, men EMD godtok ikke at det i noen tilfeller var forbud mot homofil praksis også over 21 år når denne ble utført privat og med samtykke mellom de gjeldende personene. Se også Modinos mot Kypros av 22. april 1993.

Dommen er siden blitt fulgt opp av saker som vurderer lignende reguleringer på andre områder, som A.D.T. mot Storbritannia av 31. juli 2000 (filminnspilling) og Smith og Grady mot Storbritannia av 27. september 1999 (innen Forsvaret). Spørsmål om selvskading gjennom sadomasochisme har vært oppe i blant annet Laskey, Jaggard og Brown mot Storbritannia av 19. februar 1997. Her glir en fort over i spørsmål knyttet til ytringsfrihet, som ved seksuelt eksplisitte filmer og bilder, eller spørsmål knyttet til retten til utdanning i forhold til undervisning og pedagogisk materiell.

FNs menneskerettighetskomité har nølende fulgt EMD i disse sakene, som i saken Toonen mot Australia (Communication No. 488/1992, U.N. Doc CCPR/C/50/D/488/1992 (1994)).

En annen vinkling på disse sakene, er registrering og oppbevaring av informasjon vedrørende straffedømte i sedelighetssaker. I utgangspunktet vil slik registrering være et inngrep i retten til respekt for privatliv, men myndighetene vil ha store muligheter for å rettferdiggjøre inngrepet etter artikkel 8(2) (som i Adamson mot Storbritannia av 26. januar 1999). Hvordan slik informasjon deretter benyttes, kan føre til nye problemstillinger i forhold til retten til respekt for privatliv.

3.2.20 Unntaksmuligheter

Menneskerettigheter er formulert som en motsetning: På den ene siden har individene en vidtfavnende rettighet eller frihet, på den andre siden har myndighetene ofte anledning til å beskjære rettighetene. Denne motsetningen er tydelig for en del av de sivile og politiske rettighetene, også bestemmelsen om privatliv. Her har statene uttrykkelig hjemmel til å gjøre inngrep i rettighetene: rettigheten oppstilles i første ledd og inngrepshjemmelen i annet ledd. Her stilles det tre krav: Inngrepet må ha grunnlag i lov, det må søke å nå visse oppstilte formål, og det må være nødvendig i et demokratisk samfunn.

Lovgrunnlaget volder sjelden problemer for myndighetene. Dette favner uskreven rett (som sedvanerett eller domspraksis) på linje med skreven rett (som lover og forskrifter). Det stilles krav om at loven er tilgjengelig og tilstrekkelig presis. Skjønnsmessige og vage lover er godtatt i utgangspunktet, men EMD vil foreta en konkret vurdering.

Formålene som nevnes i bestemmelsene, varierer med de ulike rettighetene. De favner temmelig vidt. Dersom myndighetene er oppmerksomme på disse formålene, vil de fleste tiltakene kunne formuleres slik at de passer inn i konvensjonens krav. Det er svært sjelden av EMD ikke godtar statenes argumentasjon her.

Kravet om at inngrepet må være nødvendig i et demokratisk samfunn, kan være mer komplisert. Mange saker står og faller med utfallet av nettopp denne vurderingen. De internasjonale tilsynsorganene kan ikke overprøve de nasjonale myndighetene fullt ut i dette spørsmålet. Myndighetene gis derfor en skjønnsmargin. Myndighetene kjenner de nasjonale forholdene bedre enn de internasjonale tilsynsorganene gjør, og det er ikke meningen at tilsynsorganene skal operere som en full fjerdeinstansordning. Tilsynsorganene vil likevel kunne overprøve dette der skjønnet ikke er utført rimelig, aktsomt og i god tro. At inngrepet er nødvendig i et demokratisk samfunn, innebærer at det må grunnes i et presserende samfunnsmessig behov. På den annen side stilles det ikke krav om at inngrepet må være uunnværlig. Det blir fort avgjørende om statene har gitt en relevant og tilstrekkelig begrunnelse for det inngrepet som gjøres.

Disse unntaksmulighetene følger av konvensjonene, også privatlivsbestemmelsen i EMK. Siden EMK er del av menneskerettsloven, vil det samme unntaksregimet anvendes for norske rettsforhold.

3.3 Oppsummering

Ovenfor har vi vist bredden i de temaene som omfattes av personverns/privatlivsbestemmelsen i EMK artikkel 8 og SP artikkel 17. Bredden i bestemmelsene følger av ordlyden i de to artiklene, hvor de fire underbegrepene (privatliv, hjem, familieliv og korrespondanse) alene og sammen (som en opphøyet personverns/privatlivsnorm) dekker et vidt spekter av forhold knyttet til enkeltpersoners integritet, intimitet og selvutfoldelse. I tillegg kommer at EMD her som for de øvrige bestemmelsene i konvensjonen, har kompetanse til å avgjøre enkeltsaker med folkerettslig bindende virkning, og at FNs menneskerettighetskomité har kompetanse til å behandle individklager (for de statene som har sluttet seg til tilleggsprotokollen til SP). Praksisen fra disse to konvensjonsorganene har bidratt til ytterligere detaljering av bestemmelsene. I tillegg har begge konvensjonsorganene til en viss grad utviklet begrepenes rekkevidde gjennom dynamisk tolkning.

Begrepene personvern/privatliv vil i en menneskerettslig sammenheng omfatte de forholdene som er skissert ovenfor. Norge vil som part til EMK og SP være folkerettslig bundet av denne forståelsen. Siden EMK artikkel 8 og SP artikkel 14 er inkorporert i norsk rett gjennom menneskerettsloven, er disse begrepene allerede tatt i bruk i norsk rettsanvendelse, og er gjennom menneskerettslovens trinnhøydebestemmelse i alle fall i teorien gitt en forrangsrett. Disse to forholdene vil gi føringer på hvilket rettslig innhold en eventuell bestemmelse om personvern/privatliv i Grunnloven burde ha.

4 Konsekvensanalyse

4.1 Synliggjøring av personvern/privatliv som sentrale verdier ved lovgivning og rettsanvendelse

Som vist ovenfor i punkt 2, er reguleringen av personvern/privatliv i de internrettslige norske kilder utpreget kasuistisk. Noen lover og enkeltbestemmelser har riktignok sikring av personvern/privatliv som særlig formål, men for mange bestemmelser er sikring av personvern/privatliv kun en sekundæreffekt som viser seg i en bestemt situasjon, jf. ovenfor i punktene 2.2.5 og 2.3. Som vist ovenfor i punkt 3.2 har svært mange

rettsspørsmål en side mot personvern/privatliv, også spørsmål det ikke er tradisjon for å anse som spørsmål om personvern/privatliv etter norsk rett. Dette innebærer at hensynet til personvern/privatliv ikke vektlegges tilstrekkelig under lovgivningsprosessen, samt ved den videre anvendelsen av reglene mellom private, i forvaltningen og i domstolene. Samtidig berører bestemmelser om personvern/privatliv grunnleggende personlige rettsforhold som det i mange tilfeller vil være sterke individuelle oppfatninger om, men ofte uten at slike diskusjoner løftes opp til det prinsipielle nivået som vil kunne ligge i privatlivsbegrepet.

En grunnlovsfesting av retten til personvern/privatliv ville medvirke til at hensyn til personvern/privatliv kommer til sin rett både i lovgivningsprosessen og ved rettsanvendelsen.

4.2 Balansering av Grunnlovens rettighetsvern: Ytringsfriheten og personvern/privatliv

Det kanskje sterkeste argumentet for å gi en grunnlovsbestemmelse om personvern/privatliv, er det forhold at ytringsfriheten – som i mange situasjoner fremstår som personvernets motpol – er gitt beskyttelse i Grunnloven. I tillegg til å utgjøre en av ganske få individuelle rettigheter som ble beskyttet allerede ved Grunnlovens vedtakelse i 1814, har ytringsfrihetsbestemmelsen nylig gjennomgått en omfattende revisjon og modernisering.

Som tematisert ovenfor under punkt 2.2.3 utgjør ytringsfrihetsbestemmelsen i Grunnloven en type negativ regulering av personvern/privatliv: Ved å kodifisere hvordan ytringsfriheten er vernet, kodifiserer man i noen grad også hvordan personvern/privatliv ikke er vernet. Denne formen for negativ regulering er imidlertid høyst ufullstendig. Ved å angi hva som ikke er vernet, angis ikke hva som er vernet.

For det tilfelle at vi er utenfor området for Grunnloven § 100, må et vern av personvern/privatliv bygges på et annet rettsgrunnlag enn en antitetisk slutning fra Grunnloven § 100.

Videre skaper kodifikasjonen av den ene rettigheten en grunnleggende ubalanse som kommer til uttrykk i den såkalte avveiningen som må foretas når det er konflikt mellom rettighetene. Når en kodifisert regel er i tilsynelatende motstrid med en antatt ukodifiserte regel, er det ingen tradisjon for å tolke den kodifiserte regelen innskrenkende. I særlig grad må dette sies å gjelde dersom de to normene i utgangspunktet må sies å ha samme ideologiske fundament eller rang. Det som i stedet gjerne skjer i slike tilfeller, er at rettsanvender viker tilbake for å gi den ulovfestede regelen et innhold i strid med den lovfestede regelen, eventuelt at rettsanvender tolker den ulovfestede regelen innskrenkende. For avveiningen mellom en generell grunnlovsfestet regel om ytringsfrihet og en ulovfestet regel om personvern/privatliv, innebærer dette at ytringsfrihetsbestemmelsen aldri vil bli tolket mot sin ordlyd i tilfeller der det er mulig konflikt med en eventuell ulovfestet norm om privatlivets fred. Konsekvensen av dette er at personvernet primært får en rolle å spille i spørsmål der ytringsfrihetsbestemmelsen enten er uklar eller uten betydning for det foreliggende rettsspørsmål. Ubalansen i Grunnloven tilsier således at ytringsfriheten sjelden vil måtte tåle korreksjon som følge av konflikt med grunnleggende personvernhensyn; disse hensynene vil primært spille en presiserende og utfyllende rolle.

Ved å gi en grunnlovsbestemmelse til beskyttelse av personvern/privatliv, hadde denne ubalansen blitt oppveid. Rettsanvender ville da fått et klart signal om at lovgiver vurderte disse forholdene som like beskyttelsesverdige rettslig og ideologisk, og at utfallet av en avveining ved eventuell konflikt på ingen måte var gitt en gang for alle.

Nå kan det hevdes at forholdet mellom de to bestemmelsene allerede ble vurdert ved revisjonen av Grunnloven § 100, slik at bestemmelsen gir uttrykk for et balansert syn på forholdet mellom ytringsfrihet og personvern/privatliv, jf. Ytringsfrihetskommisjonens utredning der nettopp analysen av personvern/privatliv står sentralt (eksempelvis NOU 1999: 27, s. 27-31). En slik slutning ville imidlertid være forhastet. Ytringsfrihetskommisjonen legger nemlig til grunn at ytringsfriheten og privatlivets fred gjelder i henholdsvis den offentlige og den private sfære. Ved å betrakte disse rettighetene som tilhørende hver sin sfære, oppstår heller ikke konflikter mellom rettighetene i den form vi har beskrevet ovenfor. Dette medfører igjen at Ytringsfrihetskommisjonen gjennom sitt forslag til «nye» Grunnloven § 100 ikke har tatt sikte på å regulere avveininger av disse rettighetene der de kolliderer innenfor en og samme sfære. (Se også punkt 1.8 ovenfor.)

Som vi kommer tilbake til nedenfor i punkt 4.3, er den sfæretenkningen Ytringsfrihetskommisjonen legger opp til problematisk, og den har heller ikke blitt fulgt opp i senere praksis og teori knyttet til Grunnloven § 100, jf. eksempelvis Rt. 2007, s. 687 og Borvik: Personvern og ytringsfri-

dom (2008, s. 5). Det er imidlertid et faktum at nye Grunnloven § 100 ligger nær opp til det Ytringsfrihetskommisjonen foreslo, et forslag som var preget av forutsetningen om de to sfærene. Når den nevnte læren om de to sfærene ikke følges opp i praksis eller teori, blir den avveiningen mellom ytringsfrihet og privatlivets fred som tilsynelatende er negativt regulert gjennom § 100, tilsvarende feilslått.

Den konstitusjonelle rettskildesituasjonen fremstår på denne bakgrunn som uheldig når privatlivets fred må avveies mot ytringsfriheten, og det kan dermed slås fast at en eventuell grunnlovsfesting ikke bare vil ha pedagogisk betydning; i alle tilfeller der ytringsfrihetsinteresser brytes mot hensynet til privatlivets fred vil en slik bestemmelse spille en vesentlig rolle for de rettslige overveielsene som foretas, og i stor utstrekning antar vi videre at en grunnlovsfesting av privatlivets fred også vil kunne få betydning for utfallet i et betydelig antall tilfeller. Under dagens rettskildetilstand vil det være vanskelig å tenke seg at hensynet til privatlivets fred vinner frem om det ikke følger av begrensninger i Grunnloven § 100 selv.

4.3 En demokratifremmende eller - hemmende effekt?

I forarbeidene til Grunnloven § 100 reflekteres som nevnt et skille oppstilt i teorien – og i utenlandsk rett – mellom den private og den offentlige sfære, slik at ytringsfriheten relaterer seg til den offentlige sfære, mens privatlivets fred relaterer seg til den private sfære (NOU 1999: 27 s. 27-31). Mens ytringsfriheten er en sentral forutsetning for demokratiet, kan ikke tilsvarende påstås med hensyn til privatlivets fred. En tilstand uten beskyttelse av privatlivet ville bl.a. innebåret en ytterligere differensiering av den offentlige samtalen; en differensiering som enkelte vil betrakte som en type «forurensing» (jf. Aarli: Vern av privatlivets fred (TfR 2005, s. 557)).

Et slikt «forurensingssynspunkt» – som innebærer at demokratiet ikke får optimale vekstvilkår om den private samtalen skal få invadere den offentlige samtalen – utgjør et argument for å sikre privatlivets fred og derved også sørge for rensing av den offentlige meningsutveksling og demokratiets vekst. Det naturlige spørsmålet i forlengelsen av dette er om slik sikring av den offentlige samtalen kan gjøres på annet vis enn gjennom grunnlovsendring. Ettersom resonnementet forutsetter et skille mellom en offentlig og en privat sfære, slik at ytringsfriheten refererer seg til den offentlige sfære, er dette høyst tvilsomt. Skillet mellom den offentlige og den private sfære er nemlig ikke sporbart i ordlyden til Grunnloven § 100, og det legges verken til grunn i nyere praksis eller juridiske teori at Grunnloven § 100 skal fortolkes på basis av et slikt skille, jf. eksempelvis Rt. 2007, s. 687 og Borvik: Personvern og ytringsfridom (2008, s. 5).

Dersom en legger til grunn at det eksisterer et skille mellom den offentlige og den private sfære, og en ønsker rensing av den offentlige samtalen i demokratiøyemed, synes således grunnlovsfesting av privatlivets fred å være riktig vei å gå. Spørsmålet blir etter dette om en bør legge til grunn et skille mellom en offentlig og en privat sfære, slik at ytringsfriheten refererer til den offentlige sfære og privatlivets fred til det private sfære.

Skillet mellom en offentlig og en privat sfære synes dels å ha referanse til en faktisk kontekst, og dels å ha referanse til utsagn av et visst innhold – antakelig fordi det forutsettes at utsagn av et visst innhold naturlig hører hjemme i en bestemt «sfære»: Når det påstås at den frie, offentlige samtalen er en forutsetning for demokratiet, og at denne samtalen vil kunne bli forurenset av utsagn som hører hjemme i den private sfære, så bygger dette på en forutsetning om at utsagnene innenfor den offentlige sfære materielt sett har et annet innhold enn utsagnene innenfor den private sfære. Denne forutsetningen viser seg å være feilslått idet det ikke er noen prinsipiell forskjell mellom den dannelsesprosessen som finner sted som følge av samtaler i det private rom, og den meningsdannelsen som finner sted som følge av samtaler og meningsutveksling i det offentlige rom. Når det påstås at samtaler fra det private rom vil forurense den offentlige kommunikasjonen om den ble viderebrakt i det offentlige rom, er dette ut fra en forutsetning om at utsagn fremsatt i private rom er mindreverdige.

Ytringsfrihetskommisjonen hevder at privatisering av det offentlige er «skadelig, ikke bare fordi det bryter med en rett til privatliv, men fordi den korrumperer den offentlige samtale slik at denne ikke kan fungere etter forutsetningen, men forfaller til sladder» (NOU 1999: 27, s. 29). Det er imidlertid ingenting ved samtalene som faktisk finner sted innenfor henholdsvis det private og offentlige rom som tilsier at denne formen for innholdsmessig rangering. Innenfor det offentlige og private rom finner alle typer samtaler sted, og det er slett ikke sikkert privatsfæren er den sfæren

der det sladres mest og hvor den «korrumperende» virksomheten primært finner sted. Muligens er det motsatt: Når den private sfære invaderes av de temaene som forefinnes i det offentlige rom «korrumperer den private samtale slik at denne ikke kan fungere etter forutsetningen som basis for dannelse, men forfaller til sladder», for å vri litt på Ytringsfrihetskommisjonens formulering. Ved å vise til den offentlige og private sfære som sfærer preget av henholdsvis demokratifremmende og korrumperende utsagn, pekes det på ideelle størrelser der kommunikasjonens innhold er styrende for hvilken sfære kommunikasjonen ideelt sett hører hjemme i. Ved å hevde at privatlivets fred gjelder for den private sfære, og ytringsfriheten gjelder i den offentlige sfære – begge sfærer gitt et ideelt innhold ut fra kommunikasjonens innhold – har Ytringsfrihetskommisjonen således ikke sagt noe annet og mer enn at den høyverdige kommunikasjonen vernes av ytringsfriheten og at den mindre høyverdige kommunikasjonen kan tåles så lenge den lever et usynlig liv i det dunkle.

Den systematikken Ytringsfrihetskommisjonen her legger opp til, er begrepsmessig sirkulær og derved uegnet som grunnlag for å angi ytringsfrihetens grenser; å innrømme noen «ytringsfrihet» etter at de materielt sett uønskede utsagnene først er luket ut, innebærer ingen reell ytringsfrihet da metoden ville passet utmerket for hvilken som helst despot. Hensynet til demokratiet tilsier således ikke at det opprettholdes et skille mellom en offentlig og privat sfære. Et slikt skille ville fungert dersom en ønsket å operere med en formell – ikke reell – rettighet kalt «ytringsfrihet» innenfor et despoti der det var et poeng at de uønskede ytringene ble fjernet før de slapp inn i «ytringsfrihetens rom».

Ettersom systematikken med et skille mellom den offentlige og private sfære ut fra kommunikasjonens innhold og ideelle rom ikke bør opprettholdes, synes det tvilsomt om en grunnlovsfesting av privatlivets fred vil styrke demokratiet. Vi deltar til enhver tid i et bredt spekter av samtaler, og grunnlovsendring er neppe veien å gå for å gjøre de offentlige samtalene mer høyverdige.

Det flere relasjoner mellom demokrati og personvern/privatliv enn den som direkte berører ytringsfriheten. Retten til respekt for privatliv innebærer blant annet at enkelpersoner står fritt i forhold til valg av studier og yrkesvei, at de kan leve ut sine politiske oppfatninger, at de kan synliggjøre sin seksualitet og seksuelle legning, at de kan uttrykke sin personlighet gjennom kles- og forbruksstil, at de selv kan velge personkrets de omgås etc. Vern om personvern/privatliv vil også ha betydning for hvilke terskler samfunnet oppstiller for deltakelse i den frie debatten, og i hvilken grad samfunnet oppfattes som reelt inkluderende og mangfoldig. En ytterligere relasjon er at mange av de samfunnsendringene som skjer gjennom demokratiske beslutninger nettopp vil regulere forhold som omfattes av personvern/privatliv (som for eksempel debatter om selvbestemt abort, overvåkning som følge av terrortrusler, likestiling av gifte og samboende par etc.). Et demokrati som ikke i tilstrekkelig grad verner om personvern/privatliv, vil dermed kunne bli et abstrakt demokrati.

4.4 Sedimentering av rettighetens innhold. Undertrykking av det dynamiske aspektet

Den tradisjonelle dualistiske betraktningsmåten innebærer at de folkerettslige forpliktelsene må transformeres eller inkorporeres for å få direkte virkning etter sitt innhold i norsk rett. Fordelen med inkorporasjon, som er fremgangmåten i menneskerettsloven, likestillingsloven og diskrimineringsloven, er blant annet at de dynamiske elementene knyttet til rettighetene til enhver tid følger med.

Det dynamiske elementet handler ikke først og fremst om at regelen korrigeres eller endres gjennom utvikling i det internasjonale kildematerialet, men at regelen presiseres og tilpasses andre elementer i rettssystemet. En grunnlovsfesting innebærer at rettigheten ikles en statisk språklig form.

Dersom en ønsker at rettigheten skal være utviklingsdyktig og dynamisk til tross for den fikserte språklige formen, må rettigheten typisk gis en vag og standardpreget form eller den må knyttes opp mot eksterne forhold som bærer dynamikken. Den vage formen gjør det riktignok mulig for de nasjonale domstolene å bruke sitt skjønn til å trekke den nærmere grensen for rettighetens nedslagsfelt, for eksempel i tilfeller der en rettighet står mot en annen. På den annen side vil den vage formen også kunne ha den effekten at domstolene blir tilbakeholdne med å utlede rettigheter fra bestemmelsen. I tilfeller der regelen er utpreget vag, kan det fremstå som nærliggende å anse regelen som en retningslinje for lovgiver, og ikke som en bestemmelse som kan danne basis for sensur av formell lov. Denne retningslinjeeffekten er altså en konsekvens av regelens språklig vage form.

Som nevnt vil en mer presis og regelpreget språklig utforming av rettigheten også virke sedimenterende: Ved å presisere språkbruken slik at skjønnsmarginen ved anvendelse av normen minker, fikseres eller låses også rettighetens innhold i et tidsmessig perspektiv: Det blir vanskeligere å tilpasse rettighetenes innhold til endringer av faktisk, normativ og kulturell art. Både i tilfeller der den internasjonale menneskerettigheten styrkes eller svekkes, og i tilfeller der den internasjonale rettigheten presiseres i forhold til andre rettigheter, vil Grunnlovens regulering være opphav til internrettslig forvanskning og rettsusikkerhet. I valget mellom en presis, regelpreget utforming og en vag, retningslinjepreget utforming synes det siste å være å foretrekke i den utstrekning den grunnlovsfestede rettigheten presiseres i forarbeider eller i formell lov. Men her vil det også spille inn i hvor stor grad den normen som inkluderes i Grunnloven er forankret i eksternt rettsmateriale. Eksempelvis vil en bestemmelse som klart bygger på bestemmelser som allerede finnes i menneskerettighetskonvensjoner som Norge har sluttet seg til, lettere kunne tolkes dynamisk enn en bestemmelse som ikke har en slik eksternrettslig forankring.

Til dette kommer det forhold at forarbeider til grunnlovsbestemmelser ofte er svært knappe (eksempelvis ved innføringen av en verdigrunnlagsbestemmelse i Grunnloven, som er blitt fremforhandlet gjennom et tverrpolitisk forlik i forbindelse med revisjon av forholdet mellom staten og Den norske kirke). På grunn av de strenge prosedyrereglene for grunnlovsendring i Grunnloven § 112 bør det dessuten fremsettes flere alternative forslag. Det er sjelden mer enn ett av disse forslagene er gitt en grundig begrunnelse fra en utredende komité. Uansett vil det kunne være større grunn enn ellers til å stille representativitetsspørsmål ved forarbeidene som uttrykk for lovgivers vilje. Årsaken til dette er til dels at forarbeidene er utpreget teoretiske og tidvis kryptiske, samt at mengden av alternative utforminger forvansker identifikasjon. Begge disse forholdene forvansker bruken av Ytringsfrihetskommisjonens utredning (NOU 1999: 27) som forarbeid.

Det faktum at vi får på plass en grunnlovsbestemmelse gjør det mindre aktuelt å vedta en utfyllende lovbestemmelse da dette vil oppfattes som både problematisk og unødig. Det problematiske består i at en risikerer å gi en lov som i en eller annen forstand ikke bare utfyller og presiserer grunnlovsbestemmelsen, men også står i direkte motstrid til denne. Det vil også være en tendens til å anse en eventuell utfylling som unødig da domstolene uansett har kompetanse til å trekke opp de nærmere grenselinjene. Det ville for eksempel være nær utenkelig å vedta en alminnelig lov om ytringsfrihet for å utfylle Grunnloven § 100.

Det finnes en mulighet for en mellomløsning mellom det å gi den eventuelle grunnlovsbestemmelsen en relativt presis, regelpreget utforming, og en vag, retningslinjepreget utforming. Mellomløsningen går ut på å gi en fanebestemmelse med retningslinjepreg som følges opp med presiserende normer med økt innslag av regelpreg. Vi finner spor av denne strukturen i Grunnloven § 100. Det problematiske med denne fremgangsmåten er at de presiserende normene kan oppfattes som en type uttømmende regulering av den rettighetspregede rettigheten. Det har på denne basis eksempelvis blitt hevdet at Grunnloven § 100 annet ledd, annet punktum er eksempel på en slik uttømmende regulering av ytringsfrihetens grense, slik at personvernssynspunkter av den type som ble lagt til grunn i dommen Rt. 1952, s. 1217 (To mistenkelige personer) ikke ville være mulig å gi gjennomslag under dagens utforming av Grunnloven § 100, jf. Moltumyr Høgberg: «Nye» Grunnloven § 100 (Lov og Rett 2006, s. 480). Dette forholdet peker imidlertid mot et annet allment problem ved grunnlovsfesting av menneskerettigheter, nemlig faren for undertrykking av det som uten regulering ville utviklet seg uten bestemmelsen. Dette er tema i neste punkt.

4.5 Undertrykking av ikke-kodifiserte rettigheter

Ovenfor i punkt 4.1 viste vi hvordan kombinasjonen av grunnlovsfestet ytringsfrihet og ikke-grunnlovsfestet vern av privatlivets fred kan medføre undertrykking av privatlivets fred i tilfeller der hensynene brytes mot hverandre. I dette punktet løftes blikket ytterligere, og vi fokuserer på hvordan en eventuell grunnlovsfesting av personvern og privatlivets fred kan tenkes å virke undertrykkende for andre ikke-kodifiserte rettigheter. Eksempel på prinsipper som kan tenkes svekket dersom retten til personvern/privatliv alene grunnlovsfestes, er det vi ovenfor i punkt 2.4 har kalt det utvidede legalitetsprinsippet.

Til tross for at man ved kodifisering av et gitt sett med menneskerettigheter ikke har til hensikt å hevde at det ikke finnes andre rettigheter, er det et faktum at fokus i særlig grad trekkes mot kodifikasjonen, slik at andre rettigheter i det minste søkes relatert til de kodifiserte rettighetene. Det-

te innebærer at rettigheter som kan konstrueres som en fortolkning av en allerede kodifisert rettighet er mer nærliggende enn det som eventuelt må oppstilles på siden av de kodifiserte rettighetene. Dette skyldes at det kodifiserte i en forstand oppfattes som sikrere, mer tilstedeværende og dermed mer «virkelig» enn det uskrevne. De tradisjonelle tolkningsresultatene basert på de skrevne kildene vil således bli foretrukket fremfor mer frirettslig utfylling av lakuner.

Også innenfor tolkningsresultatene er det mulig å se argumentative strukturer. Dersom vi står ovenfor tilsynelatende kolliderende kodifiserte rettigheter vil det være nærliggende å tolke den ene rettigheten «innskrenkende». Hvilken av de kolliderende rettigheter som skal tolkes innskrenkende, er det vanskelig å si noe allment om, muligens med unntak av en formel i forlengelse av det vektforhold Høyesterett sluttet seg til i Rt. 1976, s. 1 (Kløftaskjønnet), slik at regler som verner om personlig frihet og integritet gis forrang fremfor regler som verner om økonomiske goder.

Dersom en kodifisert regel derimot strider mot en antatt ulovfestet regel, er situasjonen klarere: Den lovfestede regelen legges til grunn etter sin ordlyd, og den ulovfestede regelen gis en fortolkning slik at konflikt ikke oppstår. Dersom det oppstår spørsmål om man er vernet av en ulovfestet regel på siden av den lovfestede, vil det være en tendens til at man som rettsanvender oppfatter problemstillingen som om den foreliggende regelen skal tolkes antitetisk eller analogisk. En slik nærliggende oppfattelse vil eventuelt sette den tredje mulige fortolkningen ut av spill: Nemlig at det utenfor regelen finnes en annen, ulovfestet regel som ikke bør oppstilles pr. analogi, altså et rent tilfelle av utfylling. Bare unntaksvis skjer slik utfylling så lenge man har en skriftlig regel å forholde seg til.

Denne tendensen tilsier forsiktighet ved spredt kodifisering.

4.6 Det høye abstraksjonsnivået reduserer ordlydens normeringsmulighet

I forlengelsen av problemet med sedimentering av ordlydens løsning ovenfor i punkt 4.4, undersøkte vi svakheter og styrker som fulgte med hhv. en klar og regelpreget utforming, og en vagere, retningslinjepreget utforming av ordlyd. Mens fokus der var lagt til ordlydens kvaliteter, rettes her fokus mot en annen side av bestemmelsen med betydning for dens normeringsmulighet; nemlig dens generalitetsnivå. Jo flere og mer forskjellige gartede kontekster en og samme bestemmelse skal regulere, jo høyere er bestemmelsens generalitetsnivå.

Regler med et høyt generalitetsnivå og med et meget omfattende potensielt nedslagsfelt vil ha retningslinjekarakter selv om ordlyden trekker i retning av at vi står ovenfor en regel. Et eksempel i denne forbindelse er Grunnloven § 97, som etter sin ordlyd griper inn i lovgivers kjernevirksomhet. Dette innebærer at den reelle vurderingen av grensen mellom den lovlige og ulovlige tilbakevirkningen må skje etter en helhetsvurdering der ordlyden bare inngår som ett av flere elementer. Tilsvarende er det med Grunnloven § 96, som sier at ingen kan (straffe)dømmes «uden efter Lov». Dette innebærer ikke at tradisjonelle rettskildefaktorer som forarbeider, rettspraksis og reelle hensyn ikke kan spille en rolle når grensen mellom straffbare og straffrie handlinger skal trekkes, men at disse sammen med ordlyden inngår som momenter i en helhetsvurdering når det skal bedømmes om tilstrekkelig hjemmel i lov foreligger. Det er ikke utenkelig at straff lovlig kan idømmes selv om dette synes å stride mot ordlyden i en aktuell straffebestemmelse, all den tid straffedommen kan knyttes opp mot («forankres i») et konkret straffebud.

Som nevnt i punkt 2.1 omfatter «personvern»/«privatliv» en rekke – delvis overlappende – underbegreper som «personlighetens rettsvern», «personregistervern» og «privatlivets fred». Disse underbegrepene kan igjen spaltes i underbegreper med referanse til ulike interesser. Når man opererer med begreper som refererer til et sett av mer eller mindre vage underbegreper, som igjen refererer til et sett av mer eller mindre vage underbegreper med referanse til et abstrakt interessevern, ligger det i saken at subsumpsjonselementet blir relativt åpent – og at en helhetsvurdering vil være avgjørende i det konkrete tilfellet. Denne typen helhetsvurderinger er i nyere rettsteori ansett å utgjøre en utfordring for rettsystemet ettersom de gjerne involverer mange inkommensurable elementer, slik at forutberegneligheten svekkes. Et eksempel på en mulig grunnlovsbestemmelse som på dette vis gir begrenset forutberegnelighet, er forslaget til grunnlovsbestemmelse om privatlivets fred og personopplysningsvern fra Vera Lysklætt og Odd Einar Dørum (Venstre). Denne bestemmelsen – nærmere bestemt alternativ 1 A til ny Grunnloven § 100 b – foreslås gitt følgende form:

> «Enhver har rett til respekt for privatliv og hjem.»

Det er høyst uklart hvilke virkninger en slik bestemmelse vil få. Bestemmelsen vil selvsagt ha en signaleffekt, samt kunne spille en prinsipiell rolle i tilfeller der personverninteresser står mot ytringsfrihetsinteresser. I det sistnevnte tilfelle vil bestemmelsen innebære at ytringsfrihetsinteressene, slik disse er beskrevet i Grunnloven § 100, ikke uten videre må gis forrang fremfor personverninteressene, men overlates til den helhetsvurdering som normalt vil finne sted ved overveielse av rettsspørsmål i norsk rett. Bestemmelsen gir imidlertid isolert sett svært få holdepunkter for hvordan denne helhetsvurderingen konkret vil slå ut. Bedre ville det ha vært om denne knappe setningen hadde vært klart forankret i for eksempel EMK artikkel 8, slik at det nærmere innholdet i setningen kan bygge på omfattende internasjonal rettslig teori og praksis.

Generelt vil det være en fordel om rettsystemets mange helhetsvurderinger søkes stabilisert. På områder med langvarig praksis vil praksisen i seg selv kunne innebære en slik stabilisering, ofte godt hjulpet av analyser over denne praksisen i juridisk teori. For nyere lover, gjelder det imidlertid å foreta presise normeringer uten for høyt generalitetsnivå, og avhjelpe eventuelle problemer i generalitetsnivået med normerende analyser og retningslinjer angitt i forarbeidene til en formell lov. Det antas ikke sjelden at problemet med regulering av personvern/privatliv i formell lov, er at det formelle lovs nivå ikke er egnet til overprøvelse av andre formelle lover som følge av lex superior-prinsippet.

Et alternativ til det å grunnlovsfeste et prinsipp med høyt abstraksjonsnivå, er det å lovfeste mer konkrete utslag av prinsippet. Disse konkrete utslagene kan rettsanvender anvende analogisk ettersom de er å anse som utslag av et mer generelt prinsipp. Heller ikke en slik kasuistisk fremgangsmåte synes tilfredsstillende for å komme rundt det problemet et høyt abstraksjonsnivå i alminnelighet medfører. Årsaken er at det er begrenset i hvilken utstrekning så vel lovgiver som rettsanvender vil bruke de kasuistiske utslagene av et mer generelt prinsipp analogisk. Et eksempel i denne forbindelse er måten det ble sett bort fra Grunnloven § 102 som nærliggende til analogisk slutning når hjemmelen for romavlytting i forebyggende øyemed ble vurdert vedtatt. Grunnloven § 102 har ordlyden: «Hus-Inkvisitioner maa ikke finde Sted, uden i kriminelle Tilfælde.» De legislative hensynene bak bestemmelsen tilsier med tyngde at heller ikke romavlytting i private hjem skulle være mulig annet enn ved etterforskning av kriminalitet. Like fullt – og uten særlige betenkeligheter i relasjon til Grunnloven § 102 – vedtas det altså en bestemmelse i politiloven (lov av 4. august 1995 nr. 53) § 17 d som gir adgang til romavlytting i private hjem selv om det ikke er mistanke om kriminell virksomhet, og selv om det ikke er tale om etterforskning av kriminell virksomhet. Når lovgiver i det aktuelle tilfellet ikke maktet å foreta en analogisk slutning fra Grunnloven § 102, noe som tross alt var meget nærliggende – tror vi ikke vi kan vente oss for mye av en kasuistisk metode for sikring av menneskerettigheter i fremtiden. Eksemplet viser tvert i mot at det i tilfeller av kasuistisk grunnlovsfesting skal svært lite til før lovgiver anser at vi befinner oss på siden av det vernede rettsgodet.

4.7 Formalisering av rettsanvendelsen og rettskildelæren?

Norsk rettsanvendelse og norsk rettsvitenskap brytes stadig mellom en formell og en materiell tilnærming til rettspørsmålene. En formell fremgangsmåte innebærer fokus på normers ordlyd, rangordning, kollisjonsregler, prinsipper m.v. En materiell tilnærming innebærer et særlig fokus på regelfragmentenes innhold, godhet, begrunnelse og realiseringen av bakenforliggende hensyn. Videre innebærer en materiell tilnærming at man er bevisst på – og drar særlig omsorg for – den skjønnsmessige vurderingen som preger svært mange rettsspørsmål.

Mange av de skjønnsmessige vurderingene man innenfor en formell tilnærming stilles ovenfor fremstår naturlig nok som helhetsvurderinger ettersom det innenfor helheten ikke utpeker seg en metakontekst som gir nøkkelen til – og rangordner – det hele. En materiell fremgangsmåte innebærer avvisning av at det finnes formelle formler, kollisjonsprinsipper og grep som «gir seg selv» ved løsningen av rettsspørsmål. Det er alltid tale om å velge «det formelle»; om å plukke ut noe fra helheten som gis særlig prioritet. En materiell tilnærming innebærer en normativ tilnærming til alle av rettsanvendelsens elementer, også spørsmålet om anvendelse av lex superior-prinsippet. For den formelle tilnærmingen fremstår det normative aspektet her som dekket av en hvit flekk. På denne basis velger vi å rubrisere den materielle tilnærmingen som den mest realistiske.

Debatten knyttet til menneskerettighetenes eventuelle semikonstitusjonelle nivå som følge av forrangsbestemmelsen i menneskerettsloven § 3, er i alt for høy grad preget til en formell tilnær-

ming til rettskildelæren. Fra et formelt synspunkt kan det selvsagt hevdes at lovgiver når som helt kan komme til å gi en lov i strid med menneskerettsloven, og det formelle lex posterior-prinsippet tilsier i så fall at den nye loven går foran menneskerettsloven, herunder dens forrangsbestemmelse i § 3. Fra et materielt synspunkt er imidlertid et slikt standpunkt lite fruktbart: Avveiningen må også i slike tilfeller inkludere analyser av regelens innhold og det endelige resultats fruktbarhet i en bred samfunnsmessig kontekst. Et eventuelt avvik fra forrangsbestemmelsen i menneskerettsloven § 3 måtte kreve solid støtte i rettskildefaktorer som forarbeider og ordlyd. Samtidig vil det stå i motstrid mot presumpsjonsprinsippet (se ovenfor kapittel 2.2.4). Det er i praksis nær utenkelig at Stortinget i det foreliggende politiske klima skulle foreta en slik demonstrativ handling mot FN og Europarådet. Dersom det imidlertid skulle være politisk klima på Stortinget for en slik handling, er det tvilsomt om den mulige rettslige skranken i menneskerettsloven skulle få Stortinget til å avstå fra en slik konflikt.

En skal merke seg at det ikke bare er talspersonene for det formelle lex posterior-prinsippet som nøkkel til løsningen som i debatten legger et for formelt perspektiv på rettskildelæren og rettsanvendelsen til grunn, men også talsmennene for det semikonstitusjonelle nivå. Ser en nærmere på domstolens faktiske rettsanvendelse, vil en raskt se at den enkle rangtenkning debatten om det semikonstitusjonelle nivå er uttrykk for, savner støtte i norske domstolers rettsanvendelse – det er i høyden tale om en teoretisk konstruksjon som har fått leve sitt liv uforstyrret fra praksis. Den eneste høyesterettsavgjørelsen som muligens er forenelig med en slik semikonstitusjonell rangtenkning, er dissensavgjørelsen Rt. 2000, s. 1811 (Finanger I). Dissensdommen er imidlertid å anse som et unntak fra den brede tendens, og man kan uansett ikke avlede en rettskildemessig struktur fra én avgjørelse, jf. Eng: Får prejudikatlæren anvendelse på domsargumenter vedrørende rettskildelæren?, TfR 1997, s. 21-44.

Spørsmålet her er om – og i så fall i hvilken retning – en grunnlovsfesting av personvern/privatliv vil bevege norsk rettsanvendelse og rettsvitenskap. I etterkrigstiden har det blitt gjort steg i retning av en materiell modell: Reelle hensyn har fått en stadig sterkere plass, og en aktiv leser av dommer eller juridiske lærebøker vil se at henvisninger til skjønnsmessige helhetsvurderinger også har økt vesentlig de siste 30 år.

Den som leser dommer og lærebøker der lovbestemmelse står mot grunnlovsbestemmelse, vil se at det såkalte lex superior-prinsippet ikke står særlig høyt i kurs: Rekken over dommer der grunnlovsbestemmelsen tolkes innskrenkende i forhold til sin ordlyd er lang. Riktignok er det enkelte teoretikere som forsøker å redde den gamle formelle lex superior-læren ved å vise til avgjørelsene der Grunnloven tolkes innskrenkende, som eksempler på «lex superior» som tolkningsmetode, slik at man i disse dommene – der det trinnhøyere argumentet tolkes innskrenkende før den «egentlige» kollisjonen – i virkeligheten representerer utslag eller anvendelse av lex superior. Vår oppfatning er at slike fremstillinger ikke er holdbare, og at lex superior-prinsippet ikke har det gjennomslaget som stundom påstås: Heller ikke et «lex superior-prinsipp» kan være noe annet og mer enn et element blant flere i en skjønnsmessig helhetsvurdering.

Det å grunnlovsfeste personvern/privatliv, kan forstås som en tilslutning til et formelt, rangmessig rettsystem der kollisjoner mellom normer på ulike «nivåer» enkelt løses ved anvendelse av et formelt lex superior-prinsipp. Dersom man forstår grunnlovsfestingen som en alminnelig tilslutning til en nyformaliseringstendens i norsk rettsanvendelse og rettsvitenskap, bør man tenke seg om to ganger før man søker grunnlovsfesting.

Etter vårt syn er imidlertid en slik fortolkning ikke noen nødvendighet. Lex superior-prinsippet er særlig knyttet til Hans Kelsens rettsteori. Denne teorien – utviklet på første halvdel av det forrige århundre – har klare begrensninger både med hensyn til det å forklare det moderne rettsystemets oppbygning, funksjonsmåte og de reelle maktforholds betydning, svakheter som etter vårt syn også gjenfinnes i lex superior-prinsippet. Det å grunnlovsfeste personvern/privatliv, trenger med andre ord ikke bety noe annet og mer for rettsanvendelsen og rettskildelæren enn at disse hensynene og verdiene sikres en sentral plass ved videre lovgivning og rettsanvendelse, jf. ovenfor i punkt 4.1.

Etter vårt syn innebærer en grunnlovsfesting av personvern/privatliv ikke noen form for tilslutning til en formalisering av norsk rettsanvendelse og rettsvitenskap, noe som igjen innebærer at vi på dette punktet ikke ser mothensyn til en eventuell grunnlovsfesting. Samtidig er det klart at det vil spille en rolle i praksis om retten er nedfelt i Grunnloven eller ikke ettersom en grunnlovsfesting vil bevirke at hensynene kommer til sin rett ved videre lovgivning og rettsanvendelse.

4.8 Pedagogisk og politisk betydning

Grunnloven har relativt stor rettslig betydning også i dag, slik vi har redegjort for i flere av underpunktene ovenfor.

Tilsvarende har Grunnloven en viktig politisk betydning. Grunnloven som politisk dokument har stor symbolkraft, noe som blant annet synliggjøres i Stortingets såkalte grunnlovskonservatisme. Den politiske debatten om endringer i relasjonene mellom staten og Den norske kirke, og særlig det omforente forslaget om innføring av en verdiparagraf i Grunnloven, viser at Grunnloven spiller en sentral rolle også når det kommer til konkrete saksforhold. Diskusjonene rundt revisjon av ytringsfrihetsbestemmelsen viser mye av det samme, tilsvarende i forhold til EU-medlemskap og de kravene som der stilles til stemmeflertall. Selv praksisen med å forfatte nye grunnlovsbestemmelser i gammel språkdrakt, vitner om den betydningen Grunnloven har langt ut over det rettslige.

Et annet nivå er den rollen Grunnloven spiller for enkeltpersoner i Norge. Feiringen av nasjonaldagen er tett knyttet opp mot Grunnloven av 1814, og Eidsvoll har en sentral plass i norsk historie og samtid. Den omfattende gaveboken som nye norske statsborgere får, vier da også Grunnloven mye oppmerksomhet. Tilsvarende er det i det opplæringsløpet som gis gjennom grunnskolen.

Et tredje nivå er den betydningen den norske grunnloven har i en internasjonal sammenheng. Det heter gjerne at vår grunnlov er den nest eldste aktive grunnloven i verden, og Grunnloven diskuteres blant annet i de menneskerettighetsdialogene Norge fører med Indonesia, Kina og Vietnam. Når Grunnloven leses alene, etterlates i internasjonal sammenheng et sterkt inntrykk av en grunnlov som prioriterer religionsfrihet innen en statskirkeramme, ytringsfrihet og eiendomsrett, i tillegg til mer spredte bestemmelser om valgsystem og rettssikkerhet. Vern om personvern/privatliv er kjernen i vernet om sivile og politiske rettigheter. Norges aktive innsats for å styrke menneskerettigheter internasjonalt kan i noen situasjoner bli møtt med kritikk av den prioriteringen som vår egen grunnlov dermed uttrykker.

Grunnloven som symbol spiller en annen rolle enn Grunnloven som rettskilde. Jurister har brukt mye av sin studietid til statsforfatningsretten, hvor hovedvekten igjen legges på Grunnloven som rettskilde, og kjenner derfor Grunnlovens rettslige styrke og svakhet på en annen måte enn personer som ikke har gjennomført slike studier. At den norske grunnloven kun verner individuelle grunnrettigheter relativt sporadisk, kan være overraskende for mange. Tilsvarende at bestemmelsene ofte er formulert i et gammelmodig språk som krever svært god leseforståelse for at en skal kunne forstå det presise innholdet i bestemmelsene.

Vi er av den oppfatning at den rollen som Grunnloven har ut over det rent rettslige tilsier at en bestemmelse om personvern/privatliv bør inkluderes i Grunnloven. Her kan det også trekkes linjer til det relativt sporadiske vernet som er vist i underpunktene ovenfor.

5 Konklusjoner og anbefalinger

Gjennomgangen ovenfor har vist at flere hensyn med styrke taler for grunnlovsfesting av retten til personvern/privatliv. Særlig viktig er hensynet til å synliggjøre personvern/privatliv som rettslig skranke og sentral verdi ved lovgivning og rettsanvendelse, et hensyn som vi tillegger avgjørende vekt. Det legges også stor vekt på at grunnlovsfesting av personvern/privatliv vil bringe bedre balanse i Grunnlovens eksisterende rettighetsvern (særlig i forhold til ytringsfrihet, religionsfrihet og eiendom). Enkelte argumenter med mulig relevans for spørsmålet om grunnlovsfesting har vist seg å trekke i flere retninger. Dette gjelder hensynet til demokratiet og det å unngå formalisering av rettsanvendelsen og rettskildelæren. Det foreligger også hensyn som tilsier forsiktighet ved en grunnlovsfesting. I denne sammenheng kan nevnes hensynet til å unngå sedimentering av rettighetens innhold og undertrykking av ikkekodifiserte rettigheter.

Samlet sett mener vi at argumentene som taler for grunnlovsfesting gjør seg gjeldende med større styrke enn motargumentene, forutsatt at man bestreber seg på å unngå enkelte av de nevnte ulempene en grunnlovsfesting har å by på.

Det er viktig at en grunnlovsfesting av personvern/privatliv klart forankres i de menneskerettslige kjernebestemmelsene, særlig EMK artikkel 8 (slik det for eksempel legges til grunn i forhold til Grunnloven § 2 og § 100). En slik forankring vil bidra til å oppveie noen av de ankepunktene vi har vist i forhold til sedimentering av rettighetens innhold. I tillegg vil en slik forankring kunne bidra til en bedre pedagogisk utforming av grunnlovsbestemmelsen, og norske rettsanvendere vil i mindre grad måtte ta stilling til rettskonflikter knyttet til såkalte trinnhøydespørsmål (særlig mellom

Grunnloven, menneskerettsloven og de eksplisitte og implisitte reguleringene i formell lovs form), reguleringslakuner og det gjennomgripende presumpsjonsprinsippet.

Den nærmere utformingen av en slik grunnlovsbestemmelse har vi innenfor rammene av denne utredningen ikke hatt anledning til å gå inn på. De føringene som er gitt ovenfor, tilsier en rimelig balanse mellom presisjonsnivå og abstraksjonsnivå. En slik grunnlovsbestemmelse bør videre få klart frem at rettigheten ikke gjelder ubetinget, verken i forhold til andre enkeltindivider eller i forhold til samfunnets behov, gjerne langs de samme linjene som følger av EMK artikkel 8 annet ledd. Den ordningen som er inntatt i Grunnloven § 100, med en summarisk begrunnelse for rettigheten implementert i ordlyden, vil videre kunne bidra til å øke forståelsen for bestemmelsens rekkevidde både for jurister og for andre som forholder seg til Grunnloven.

Vi mener den beste løsningen ideelt sett er en revisjon av Grunnloven med sikte på å styrke individets grunnlovsvern, samtidig med at den norske statsordningen befestes og klart uttrykkes. Dagens grunnlov er etter vårt skjønn for mye preget av historiens løp og den relativt tilfeldige reguleringen på mange grunnleggende rettsområder. Grunnloven har ikke i tilstrekkelig grad tatt opp i seg de store rettslige og politiske endringene som har skjedd i vår kulturkrets de siste 60 år, og speiler verken samfunnsstrukturen eller de underliggende individrelaterte normene på en dekkende måte. Denne ideelle reguleringen vil nødvendigvis måtte ta relativt lang tid å få på plass, dels grunnet endringsbestemmelsene i § 112 og dels grunnet i de omfattende politiske diskusjonene dette vil kunne trekke med seg.

Innen en slik større grunnlovsrevisjon er fullendt, er det vår anbefaling at Stortinget grunnlovsfester retten til personvern/privatliv.

Vedlegg 4

Personvernøkende teknologi og identitetsforvaltning

Thomas Olsen
Avdeling for forvaltningsinformatikk, UiO

1 Innledning

Den teknologiske utviklingen åpner opp for stadig nye tjenester som vil kunne sette personvernet i fare. Er det gitt at ny teknologi og ny teknologianvendelse nødvendigvis må medføre redusert personvern? Eller kan det tenkes at teknologien kan designes på en måte som fremmer eller øker personvernet? *Personvernøkende teknologi* (engelsk: Privacy-Enhancing Technologies – «PETs») antyder at dette er mulig. Som vi skal se, har PETs i snever forstand omhandlet tekniske og organisatoriske tiltak som tar sikte på å begrense andres mulighet til identifisere den enkelte. Tilnærmingen bygger på utgangspunktet om at personvernhensyn kun gjør seg gjeldende dersom transaksjoner eller opplysninger kan knyttes til den de gjelder. Dette tradisjonelle fokuset på PETs som løsninger for anonymitet og pseudonymitet er fremdeles viktig. Imidlertid skal vi se at utviklingen går i retning av å betrakte disse spørsmålene om identitet og identifiserbarhet under synsvinkelen *identitetsforvaltning*. Identitetsforvaltning tar utgangspunkt i individets ulike roller og hvordan identifisering og autentisering kan tilpasses disse rollene og relasjonene. I det følgende skal vi se nærmere på bakgrunnen for PETs og identitetsforvaltning, hvordan slike løsninger kan styrke personvernet, samt forholdet til det rettslige vernet om personopplysinger.

1.1 Bakgrunn

Begrepet PETs kan føres tilbake til 1995 da datatilsynsmyndighetene i Ontario (Canada) og Nederland la frem sin felles rapport «Privacy-enhancing technologies: the path to anonymity».[1] Rapporten ble presentert på den 17. internasjonale datatilsynsmyndighetskonferansen i København samme år. I følge John Borking, den gang tilknyttet Registratiekamer – senere «PETs-evangelist», skapte budskapet stor oppsikt. Rapporten viste at de fleste informasjonssystemer kan designes slik at brukerens identitet holdes helt eller delvis skjult. Nøkkelen til slik personvernøkende design var «the identity protector» – en koblingssentral hvor personidentifiserende identifikatorer (som f. eks. fødselsnummer) ble gjort om til pseudonymer som ikke direkte kunne knyttes til noen identifiserbar person. Slike koblingssentraler mellom identifiserbare identifikatorer og pseudonymer kunne plasseres i informasjonssystemets ulike deler, eller være under brukerens direkte kontroll. Videre viste rapporten hvordan slike koblinger kunne skje automatisk i systemet, eller etter nærmere bestemte regler av en uavhengig og tiltrodd pseudonymforvalter.

Den prinsipielle betraktningen om at personvernet kan ivaretas ved å begrense muligheten til identifisering var imidlertid ikke ny. Allerede i 1981 publiserte David Chaum sin banebrytende artikkel om hvordan man kunne oppnå anonymitet for avsender og mottaker av elektronisk kommunikasjon.[2] Innenfor kryptografien hadde man lenge forsket på hvordan kryptering av elektronisk kommunikasjon kunne sikre *innholdet* fra uautorisert innsyn. Chaums tilnærming var en helt annen: det faktum at noen kunne observere *hvem* som kommuniserte med *hvem* kunne være uheldig fra et sikkerhets- og personvernsynspunkt.

Også Norge kan skilte med pionerarbeid innenfor personvernøkende teknologi. Tidlig på 1990-tallet arbeidet et offentlig utvalg ledet av professor Erik Boe med hvordan man kunne forene samfunnets behov for forskning på helseopplysinger samtidig som den enkeltes personvern ble ivaretatt. Mens man tidligere hadde skilt mellom

[1] Registratiekamer, *Privacy-enhancing technologies: the path to anonymity (Vols I & II)*, 1995

[2] Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, vol. 24 no. 2, 1981

anonyme eller avidentifiserte opplysninger (som ga relativt begrensede muligheter for forskning) og fullt ut identifiserbare opplysninger (som medførte en ikke ubetydelig personvernrisiko), ble det i NOU 1993:22 «Pseudonyme helseregistre» foreslått en radikal endring i måten å organisere helseregistre på. I stedet for å lagre helseopplysinger med fødselsnummer, ble det foreslått at opplysningene skulle lagres under pseudonymer generert av en tiltrodd pseudonymforvalter. Tankegangen og prinsippet var det samme som i PETs-rapporten fra 1995: ved å bytte ut personidentifiserbare identifikatorer med pseudonymer kunne man oppnå samme funksjonalitet, samtidig som risikoen for personvernkrenkelser ble vesentlig redusert.

1.2 Forsøk på definisjon

Selv om begrepet «personvernøkende teknologi» og akronymet «PETs» er relativt kjent i miljøer som arbeider med personvernspørsmål,[3] finnes det fremdeles ingen omforent definisjon. Kjernen i begrepet har imidlertid hele tiden vært dataminimalitet, nærmere bestemt på å begrense muligheten for å identifisere den opplysningene gjelder. Dette fremkommer av Herbert Burkerts mye siterte definisjon:[4]

> "The term privacy-enhancing technologies (PETs) refers to technical and organizational concepts that aim at protecting personal identity."

Fokuset på identitet kan forklares ved at personverninteresser ikke gjør seg gjeldende dersom den opplysningene gjelder ikke kan identifiseres. Dette faktum gjenspeiles i personopplysningslovgivningen som bare gjelder i den grad det behandles opplysninger om en identifiserbar person.

I personvernkretser har det vært en debatt om kryptografi faller innenfor PETs-begrepet. Uenigheten kan skyldes at kryptografi har mange bruksområder. Benyttes kryptografi som ledd i en anonymiserings- eller pseudonymiseringsprosess, vil dette falle inn under den opprinnelige forståelsen av PETs. Er det snakk om innholdskryptering av opplysninger som kommuniseres eller som er lagret, vil dette være et rent informasjonssikkerhetstiltak. Kryptering har da som siktemål å verne opplysningene fra uautorisert innsyn (konfidensialitet) eller endring (integritet), og angår ikke identitet og muligheten for identifisering. Dette prinsipielle skillet mellom informasjonssikkerhetstiltak og PETs vil bli nærmere kommentert i eksemplet om pseudonyme helseregistre.[5]

Av deler av diskusjonen om PETs kan man få inntrykk av at PETs er avgrenset til å gjelde programvare som kan bidra til å løse personvern- og sikkerhetsutfordringer på Internett. Det er ingen tvil om at Internett medfører nye trusler som kan avhjelpes med ulike typer tekniske løsninger. Eksempler på dette er brannmurer, antivirus, antispyware, spamfilter osv. Om PETs også skal omfatte slike tekniske tiltak, som gjerne er knyttet til den enkelte brukers personlige utstyr, kan diskuteres. Jeg er av den oppfatning at slike løsninger primært knytter seg til informasjonssikkerhet, og at man med fordel bør forbeholde PETs om tekniske og organisatoriske tiltak som gjelder identitet og identifisering. Et ensidig fokus på brukerstyrte «tools» henleder tanken til at PETs er begrenset til noe som den enkelte bruker kan anvende. Som vi skal se i kapittel 3.2, vil mange av identitetsspørsmålene ved elektronisk kommunikasjon avhenge av tekniske og organisatoriske forhold knyttet til brukerutstyr, «infrastruktur» og kommunikasjonsmotpart (her kalt «tjenesteyter»).

Mens PETs-begrepet altså må anses forholdsvis innarbeidet, dog med varierende meningsinnhold, har viktige deler av forskningen og utviklingen siden begynnelsen av 2000-tallet skjedd innenfor området *identitetsforvaltning* (engelsk: identity management). Særlig har utviklingen vært drevet frem av store tverrfaglige EU-prosjekter.[6] Personvernøkende identitetsforvaltning tar utgangspunkt i enkeltindividets ulike *roller*, f.eks. ansatt, student, eller kunde, og hvordan identifise-

---

[3] For eksempel har det siden år 2000 vært avholdt en årlig internasjonal workshop om PETs, se http://petworkshop.org/.

[4] Burkert, "Privacy-enhancing technologies: typology, critique, vision", I: *Technology and privacy: the new landscape*, Agre og Rotenberg (red), 1997

[5] Se tilsvarende Burkert, "Privacy-enhancing technologies: typology, critique, vision", I: *Technology and privacy: the new landscape*, Agre og Rotenberg (red), 1997 s 125: "PETs have to be set apart from data-security technologies. It is one of the merits of the discussion on PETs that the concept of data security has been reclarified as to its limits with regard to privacy protection. Data-security measures seek to render data processing safe regardless of the legitimacy of processing. Data security is a necessary but not a sufficient condition for privacy protection. PETs on the other hand, seek to eliminate the use of personal data altogether or to give direct control over revelation of personal information to the person concerned. PETs are therefore closer to the social goals of privacy protection."

[6] Se f.eks. EU-prosjektene PRIME, GUIDE, FIDIS, PRIME-LIFE og PICOS.

ring og autentisering kan tilpasses rollene. Dette reiser spørsmål om tildeling av hensiktsmessig identifikator (f.eks. brukernavn) og autentiseringsmekanisme (f eks passord). I tillegg til å rette oppmerksomhet mot roller, har forskningen også opptatt seg med spørsmålet om muligheten for å autentisere, dvs etablere tilstrekkelig sikkerhet for, andre forhold enn identitet/roller. Ved å autentisere andre relevante *egenskaper*, f.eks. medlemskap, alder eller kjønn, vil det være mulig å tilby en lang rekke tjenester uten å knytte dette til noen identitet.[7] Deler av denne forskningen tar altså utgangspunkt i PETs-tilnærmingen og dens fokus på dataminimalitet.[8] Forskningen innenfor identitetsforvaltning har imidlertid løftet spørsmålene om identitet og identifiserbarhet opp på et nivå hvor man ikke ensidig ser på muligheten for å begrense identifiserbarhet. Vel så viktig er det å stille spørsmål med *hva* (f.eks. hvilken rolle) som skal identifiseres, og å sørge for at dette gjøres på en tilstrekkelig sikker måte (autentisering). Identitetsforvaltningsperspektivet innebærer derfor en mer helhetlig tilnærming til elektronisk samhandling hvor mange av de tradisjonelle PETs-komponentene settes sammen til mer brukervennlige løsninger. Se nærmere om sammenhengen mellom PETs og identitetsforvaltning i kapittel 3.2-3.5.

Parallelt med den akademisk forankrede forskningen har det i IT-industrien skjedd en rivende utvikling av tekniske standarder for identitetsforvaltning.[9] Motivasjonen bak dette arbeidet har særlig vært å effektivisere tilgangsstyringen til virksomheters ulike ressurser og tjenester. Bak arbeidet ligger også ønsker om å imøtekomme regulatoriske krav i forhold til informasjonssikkerhet og i forhold til å ha kontroll på hvem som har tilgang til hva. Det er slike standarder som ligger til grunn for felles tilgangsløsninger (single sign-on), slik MinSide og Altinn er eksempler på. Selv om informasjonssikkerhet og personvern er sentrale hensyn ved utvikling av standardene, vil personvernimplikasjonene langt på veg avhenge av *hvordan* disse implementeres.[10] I den forbindelse bør det nevnes at PETs av og til også benyttes om standarder og systemer som gjør det mulig for den behandlingsansvarlige å etterleve personvernlovgivningens krav. Dette er imidlertid langt fra den opprinnelige betydningen av begrepet. Til dette kan det også anføres at teknologi som er personvern*økende* bør være noe utover teknologi som «gjør det mulig» å behandle opplysninger i henhold til lovens krav. Se nærmere om systemer og standarder for identitetsforvaltning i kapittel 3.6.

Denne korte oversikten viser altså at PETs (og senere personvernøkende identitetsforvaltning) brukes om et nokså bredt spekter av tekniske og organisatoriske tiltak for å ivareta personvernet. Av den grunn er det etter min oppfatning hensiktsmessig å holde fast ved den opprinnelige betydningen knyttet til identitet og begrenset identifiserbarhet, jf. Burkerts definisjon over. Dette utelukker imidlertid ikke at PETs-begrepet – utover denne snevre betydningen – kan fungere utmerket som generell betegnelse på teknologi som er ment å ivareta personvernhensyn. Slik sett kan PETs benyttes om tekniske og organisatoriske løsninger som har blitt utviklet med en *intensjon* om å ivareta personvernet.[11] Dette understreker betydningen av at personvernspørsmål ikke er noe som kan håndteres til slutt når alle designvalg er tatt, men at personvernhensyn må vektlegges i alle trinn i utviklingsprosessen.

1.3 Politisk ønske om å fremme personvernøkende teknologi

Internasjonalt har det i en årrekke vært politisk oppmerksomhet rundt teknologiens rolle som en trussel mot personvernet, men også som en mulig strategi for å sikre personvernet. Til tross for pionervirksomhet i forhold til pseudonyme helseregistre, må det sies at bevisstheten her hjemme i forhold til PETs har vært nokså lav. Norske myndigheter har i liten grad løftet disse spørsmålene opp på dagsorden, og Datatilsynet har i liten grad arbeidet proaktivt i forhold til utvikling og anven-

---

[7] Se f.eks. Brands, *Rethinking public key infrastructures and digital certificates: building in privacy*, Cambridge, Mass. 2000, løsninger levert av selskapet http://www.credentica.com/ og arbeider av Jan Camenisch, IBM, http://www.zurich.ibm.com/%7Ejca/publications.html.

[8] Se f.eks. Hansen et al., "Privacy-enhancing identity management", *Information Security Technical Report*, 1, 2004 35-44.

[9] Særlig toneangivende har standardiseringsorganisasjonene Liberty Alliance og OASIS vært i forhold til utvikling av standarder for såkalt føderert identitetsforvaltning.

[10] Enkelte forskere har vært kritiske til denne standardutviklingen og hevder at virksomhetenes interesser i å legge til rette for nye forretningsmodeller har fått mer gjennomslag enn hensynet til brukernes personvern. Se f.eks. Clarke, *Identity Management*, 2004. Se nærmere om personvernspørsmål i forbindelse med implementering av standarder for føderert identitetsforvaltning i Olsen og Mahler, "Identity management and data protection law: Risk, responsibility and compliance in `Circles of Trust'", *Computer Law & Security Report*, 4 & 5, 2007 342-351 & 415-426 og Olsen og Mahler, *Identity management & Privacy*, Complex, 2007.

[11] Se tilsvarende Bygrave, "Privacy-Enhancing Technologies – Caught between a Rock and a Hard Place", *Privacy Law & Policy Reporter*, 2002 135-137.

delse av teknologi for å sikre personvernet. Enkelte datatilsynsmyndigheter, som f.eks. datatilsynsmyndigheten i den tyske delstaten Schleswig Holstein, det nederlandske datatilsynet (Registratiekamer), og tilsynsmyndigheten i Ontario, Canada, har utmerket seg med aktivt å forsøke påvirke teknologiutvikling og -anvendelse. Deler av arbeidet kan karakteriseres som en «strategisk entusiasme» til ny teknologi, hvor deltakelse i forskningsprosjekter og aktiv dialog med IT-industrien gjør det mulig å påvirke aktørenes bevissthet om personvernspørsmål. Slikt arbeid krever ressurser og en klar strategi for hvilken rolle tilsynsmyndigheten skal ha. Som vi skal se i kap 0 er dagens personopplysningslovgivning teknologinøytral. Lovgivningen regulerer *anvendelse* av teknologi for å behandle personopplysninger, og ikke teknologien i seg selv, noe som kan forklare at tilsynsmyndigheter ofte har liten innflytelse på selve teknologiutviklingen.

Fra EUs side er det en klar politisk vilje til å fremme PETs. I forbindelse med evaluering av medlemsstatenes implementering av personverndirektivet (95/46/EF) i 2003, ble videre satsning på PETs løftet frem som et av satsningsområdene.[12] Dette er senere fulgt opp fra EU-kommisjonen med en handlingsplan for å fremme PETs.[13] Kommisjonens strategi er for det første å fremme *utvikling* av PETs, legge incentiver for næringslivets og offentlige myndigheters *anvendelse,* samt å heve folk flest sin *bevissthet* om PETs og personvernsspørsmål.

I Norge er spørsmål knyttet til personvern og personvernøkende teknologi berørt i St.meld. nr 17 (2006-2007) («IKT-meldingen»). Av meldingen fremkommer det at Regjeringen ønsker å styrke satsningen på personvernøkende teknologi. Her er PETs beskrevet som «Teknologi som støttar opp under personvern i elektronisk kommunikasjon over Internett». Dette er en noe unyansert beskrivelse, da PETs som vi skal se ikke bare er relevant i forhold til Internett. Beskrivelsen sier heller ikke noe om *hvordan* teknologien kan styrke personvernet. Kryptering nevnes som eksempel på PETs. Som nevnt over strides det om kryptering er en sikkerhetsteknologi eller PETs. Gode grunner taler i alle fall for at man må skille mellom innholdskryptering og kryptering i forbindelse med anonymisering og pseudonymisering. For øvrig fremhever meldingen viktigheten av at det i samfunnet legges til rette for anonyme eller pseudonyme løsninger i sammenhenger der det ikke er nødvendig å identifisere seg (kapittel 8.3.3 «Retten til å være anonym»). I den forbindelse nevnes viktige områder som faller inn under kjerneområdet for PETs og identitetsforvaltning:

> «– *Pseudonyme løysingar som alternativ til full anonymitet og full identifikasjon*
> – *Pseudonyme sertifikat i løysinger for digital signatur der dette er tilstrekkeleg*
> – *Anonyme betalingskort som alternativ til bankkort/kredittkort som er knytte til identitet.»*

Det er naturlig å lese meldingen slik at ønsket om å bevare muligheten for anonymitet nødvendigvis må legge føringer for utvikling og anvendelse av teknologi. Sammenhengen mellom anonymitet/pseudonymitet og PETs/identitetsforvaltning vil bli nærmere belyst i den videre fremstillingen.

2 Pseudonyme helseregistre

Boe-utvalgets forslag til en ny registerform for lagring av helseopplysninger til forsknings- og administrasjonsformål er et godt eksempel på hvordan tekniske og organisatoriske tiltak kan bidra til å sikre personvernet. Som nevnt i innledningen tar registerformen utgangspunkt i selve grunntanken med PETs ved at opplysningene som lagres er knyttet til et pseudonym som ikke direkte kan knyttes til noen identifiserbar person.

Forslaget var nyskapende og dristig, og ble ikke helt uventet møtt med en god del skepsis. Til tross for en noe kronglete lovgivningsprosess,[14] er den pseudonyme registerformen nå tatt inn i dagens helseregisterlov.[15] Loven skiller i § 2 mellom fire opplysningstyper:

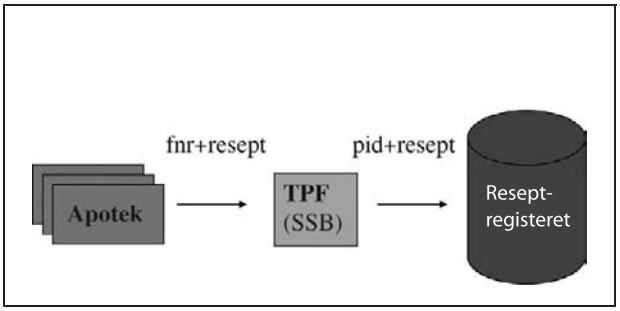
> *«helseopplysninger*: taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en enkeltperson,
>
> *avidentifiserte* helseopplysninger: helseopplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en

[12] EU Commission, *First report on the implementation of the Data Protection Directive (95/46/EC)*, 2003.

[13] European Commission, *Communication on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, 2007.

[14] Boe, "Nye helseregistre inn bakveien?" *Kritisk juss*, Årg. 27, nr 1/2, 2000 63-77. http://www.afin.uio.no/forskning/notater/6_00.html.

[15] Lov om helseregistre og behandling av helseopplysninger (helseregisterloven), lov 18. mai 2001 nr 24.



Figur: 4.1 Informasjonsflyt i reseptregisteret

enkeltperson, og hvor identitet bare kan tilbakeføres ved sammenstilling med de samme opplysninger som tidligere ble fjernet,

anonyme opplysninger: opplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson,

pseudonyme helseopplysninger: helseopplysninger der identitet er kryptert eller skjult på annet vis, men likevel individualisert slik at det lar seg gjøre å følge hver person gjennom helsesystemet uten at identiteten røpes»

Et hovedskille går mellom anonyme og avidentifiserte opplysninger, og personidentifiserbare (kalt «helseopplysninger» over) og pseudonyme opplysninger. De to førstnevnte er *ikke personentydige*, det vil si at de ikke er tilknyttet noen entydig identifikator som gjør det mulig å legge til flere opplysninger på et senere tidspunkt. Disse to opplysningstypene gir derfor begrensede muligheter for forskning, siden man ikke kan følge et individ over tid eller samkjøre dataforekomster angående samme individ fra ulike registre. Personidentifiserbare opplysninger og pseudonyme opplysninger er derimot begge personentydige. Forskjellen er at personidentifiserbare opplysninger er knyttet til identifiserbare opplysninger (typisk fødselsnummer), mens pseudonyme opplysninger er knyttet til et pseudonym som hindrer direkte identifisering av den opplysningene gjelder.

Begrunnelsen for at et pseudonymt register anses å kunne ivareta forskningens behov samtidig som personvernet ivaretas på en hensiktsmessig måte, kan illustreres med informasjonsflyten i det pseudonyme reseptregisteret, jf. figur 4.1.[16]

Apotekene registrerer reseptopplysninger og fødselsnummer på rekvirenten. Hver måned sender apotekene disse opplysningene til tiltrodd pseudonymforvalter («TPF» – i dette tilfellet Statistisk sentralbyrå (SSB)). Selve reseptopplysingene er kryptert for TPF. TPF kjører fødselsnumrene gjennom en en-veis krypteringsalgoritme som generer et entydig pseudonym. Pseudonym og tilknyttede reseptopplysninger blir så oversendt til reseptregisteret hvor opplysningene lagres. Siden krypteringsalgoritmen genererer det samme pseudonymet hver gang, vil opplysninger om nye reseptutleveringer legges til den enkeltes profil i registeret. Registeret er altså i likhet med et personidentifiserbart register *personentydig*, noe som gjør det mulig å følge enkeltindivider over tid. Forskjellen er identifikatoren som er knyttet til opplysningene. I et pseudonymt register er fødselsnummer byttet ut med et pseudonym som er generert av en tiltrodd tredjepart. I prinsippet skal derfor et personidentifiserbart og et pseudonymt register være like godt egnet til å oppfylle helseforsknings- og administrasjonsformål. Vi kommer tilbake til innvendingene mot dette utgangspunktet rett under.

Flertallet i Boe-utvalget bygget på standpunktet om at et pseudonymt register vil ivareta personvernhensyn bedre enn et personidentifiserbart register. Poenget med den pseudonyme registerformen er å sikre at de som får tilgang til opplysningene, også autoriserte personer, ikke skal kunne identifisere personen opplysningene omhandler. Risikoen for personvernkrenkelser er derfor vesentlig redusert.

I et personidentifiserbart register vil ivaretakelsen av personvernet i mye større grad avhenge av sikkerhetstiltak og tilgangskontroll. Spørsmålet om valg av registerform dukket opp igjen i forbindelse med Norsk pasientregister. Utfallet ble her et identifiserbart register med «internt krypterte identiteter». I forarbeidene til endring av helseregisterloven ble det argumentert med at personvernet vil bli tilfredsstillende ivaretatt med tradisjonelle sikkerhetstiltak som skal sikre at bare autorisert personell skal ha tilgang til de identifiserbare opplysningene.[17] Med tanke på den etablerte oppfatningen om at den største sikkerhetstrusselen kommer fra virksomheters egne ansatte, kan dette sies å være betenkelig.

Det er altså her den prinsipielle forskjellen mellom den pseudonyme og identifiserbare registerformen ligger: sikkerhetstiltak som «internt krypterte identiteter» sikrer bare mot *uautorisert*

[16] Registeret er nærmere regulert i Forskrift om innsamling og behandling av helseopplysninger i Reseptbasert legemiddelregister (Reseptregisteret), forskrift 17. oktober 2003 nr 1246.

[17] Se Ot.prp. nr 49 (2005-2006) Om lov om endringer i helseregisterloven (Norsk pasientregister).

tilgang, og løser ikke den sårbarheten som ligger i at *autorisert* personell har tilgang til identifiserbare opplysninger. Et pseudonymt register må også vernes mot uautorisert tilgang med tradisjonelle sikkerhetstiltak, men gjør registeret vesentlig mindre sårbart for misbruk fra de som faktisk er autorisert til å behandle opplysningene. Det er dette som gjør at man, etter min oppfatning, kan kalle den pseudonyme registerformen for «personvernøkende». Innholdskryptering og tilgangskontroll er bare tradisjonelle sikkerhetstiltak, jf. sondringen PETs og sikkerhetsteknologi i kapittel 1.2.

I debatten rundt Norsk pasientregister ble det brukt som argument for et identifiserbart register at den pseudonyme registerformen ikke gir like god *datakvalitet* som et identifiserbart register. Et annet argument var at et pseudonymt register gir begrenset *anvendelighet* fordi rettslige og tekniske hindre gjør det umulig å kontakte den opplysningene gjelder. Det er ikke anledning til å gå inn på disse spørsmålene her.[18] Det man kan slå fast er i hvert fall at den pseudonyme registerformen oppfattes som mer kompleks, noe som har gitt grunnlag for forvirring og skepsis fra politikere og helseforskere.[19]

3 Elektronisk kommunikasjon

3.1 Elektroniske spor og identifisering

Personverndebatten både her hjemme og internasjonalt har de senere år vært preget av nye personvernutfordringer knyttet til «elektroniske spor». Elektroniske spor er et bilde på et bredt spekter av opplysninger som typisk genereres og lagres ved bruk av ulike elektroniske hjelpemidler. Studier av personvernproblematikk knyttet til elektroniske spor viser at det siden begynnelsen av 1990-tallet har vært en drastisk økning i mengden elektroniske spor og at disse blir stadig mer innholdsrike.[20] Metodene for å analysere slike data har utviklet seg i takt med den teknologiske utvikling, og gjør det mulig å gi et nyansert bilde av gruppers eller enkeltpersoners bevegelsesmønster, omgangskrets og interesser.[21]

Forskningsresultater viser også at utbredelsen av elektroniske tjenester gjør at man som enkeltindivid i stadig større grad og på stadig flere samfunnsområder oppfordres eller tvinges til å identifisere seg.[22] Dette gjelder både for å få tilgang til kommunikasjonstjenester og i forhold til virksomheter som yter innholdstjenester som forutsetter elektronisk kommunikasjon. På visse områder er det klart at det er et legitimt behov for å kunne identifisere den man kommuniserer med eller disponerer rettslig i forhold til. Dette gjelder f eks i forhold til å sørge for at bare autorisert helsepersonell får tilgang til lagrede helseopplysninger, at en medkontrahent kan holdes ansvarlig for kontraktsrettsbrudd, eller at den som gjør seg skyldig i straffbare forhold kan identifiseres og holdes ansvarlig for sine ugjerninger. På andre områder, f eks i forhold til mange av våre dagligdagse trivielle gjøremål, kan det imidlertid tenkes at identifisering er mindre viktig.

Fra et personvernsynspunkt gir hyppigere krav til identifisering grunn til å reise prinsipielle spørsmål knyttet til om identifisering er *nødvendig*, *hva* som eventuelt skal identifiseres og *hvordan* man foretar en identifisering.

- *Nødvendig* sikter til at det i mange transaksjoner ikke er nødvendig å vite *hvem* man samhandler med. Det man egentlig trenger å vite er f.eks. alder, kjønn, medlemskap, om betalingen er mottatt, eller om vedkommende har betalingsevne og -vilje.
- *Hva* henspeiler på det faktum at vi alle har ulike roller, og at det er den relevante rollen som skal identifiseres, jf. introduksjonen til identitetsforvaltning i kapittel 1.2.

[18] Innvendingene har blitt imøtegått av Kompetansesenteret for IT i helsesektoren (KITH) og professorene Dag Wiese Schartum og Erik Boe. Dokumenter er tilgjengelig på nettsiden *Personvern på nettet* under tittelen "Åpen høring om forslaget til Norsk Pasientregister", 6. november 2006, http://www.personvern.uio.no/pvpn/nyheter.html.

[19] Forskningsresultater viser for øvrig at de pseudonyme registrene er velfungerende i praksis, men at det fremdeles hersker en del tvil om hva et pseudonymt register faktisk innebærer. Se nærmere Andresen, "On Pseudonymous Health Registers: While they Work as Intended, they are Still Controversial in Norway", *Proceedings of the First International Conference on Health Informatics, Funchal, Madeira - Portugal*, Vol 1, 2008 59-66 og L'Abée-Lund, *Pseudonymisering av personopplysninger i sentrale helseregistre*, Oslo, 2006.

[20] Se Teknologirådet, *Elektroniske spor og personvern*, 2005 og Norsk Regnesentral, *Elektroniske spor*, Oslo 2005.

[21] Se nærmere om automatisert profilering i Bygrave, *Data protection law: approaching its rationale, logic and limits*, Dortrecht 2002, s 104-105 og kapittel 17.

[22] Se f.eks. Teknologirådet, *Elektroniske spor og personvern*, 2005, s 106, Norsk Regnesentral, *Elektroniske spor*, Oslo 2005, s 65 og Kent og Millett, *Who goes there?: authentication through the lens of privacy*, Washington, DC 2003, s 30. Se også Datatilsynet, *E-forvaltning – Datatilsynets tilrådning til regjeringen*, Datatilsynets nettsted, 2007, s 6, hvor tilsynet tilråder regjeringen om at det "trekkes opp retningslinjer som sikrer at identifisering kun skjer når det er reelt behov for sådan".

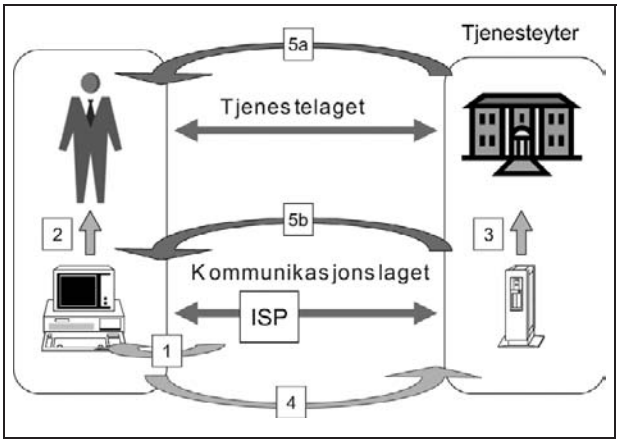
– *Hvordan* sikter til at identifiseringen må ha tilstrekkelig kvalitet slik at man f.eks. unngår forveksling og identitetsmisbruk.

Et sentralt begrep i forhold til disse spørsmålene er *autentisering*. Autentisering er en prosess som tar sikte på å etablere tilstrekkelig sikkerhet for en påstand. Påstanden kan f.eks. knytte seg til identitet, rolle eller egenskap. Eksempelvis kan en påstand om at man er over 18 år autentiseres ved å vise gyldig ID-kort i skranken. Videre kan en påstand om at man har rådighet over en bestemt brukerkonto på Internett autentiseres ved hjelp av et passord. Se nærmere om autentisering i kapittel 3.5.

I det følgende skal vi se nærmere på hvordan utfordringene knyttet til elektroniske spor, identifisering og autentisering kan betraktes som et spørsmål om *identitetsforvaltning* på Internett.

3.2 Identitetsforvaltning i tjeneste- og kommunikasjonslag

Det er innen elektronisk kommunikasjon, og spesielt Internett, at det har vært mest fokus på personvernøkende teknologi. Mye av diskusjonen har vært knyttet til enkelte brukerstyrte tekniske løsninger som kan hindre «tjenesteytere» i å oppbarbeide profiler over brukeres gjøren og laden på Internett. Vi skal her se at dette er én viktig problemstilling, men at det også er andre spørsmål som omhandler identitet og identitetsforvaltning som fortjener oppmerksomhet. Utgangspunktet for den videre fremstillingen er figur 4.2 som sondrer mellom tjeneste- og kommunikasjonslag, og som angir relasjonene mellom bruker, ISP og tjenesteyter.



Figur: 4.2 Identitetsforvaltning i tjeneste- og kommunikasjonslag

Modellen er en forenkling av informasjonsflyten mellom en bruker og en tjenesteyter på Internett.[23] Poenget er å synliggjøre at visse identitetsforvaltningsspørsmål kan knyttes til den tekniske infrastrukturen som Internett utgjør (kommunikasjonslaget), mens visse spørsmål må løses i tjenestelaget. Mens kommunikasjonslaget i hovedsak gjelder identifisering og autentisering av maskiner (brukers klient og tjenesteyters server), handler tjenestelaget om identifisering og autentisering av brukeren og tjenesteyteren. Vi skal i det følgende se nærmere på de enkelte relasjonene, og hvordan de mest omtalte PETs kan bidra til å sikre personvernet.

3.2.1 Relasjonen ISP – bruker (1) og (2)

For å kunne knytte sin datamaskin til Internett må brukeren for det første inngå avtale med en tilbyder av elektronisk kommunikasjon («ISP», nr 1 i figuren). Tilbyder av telefontjeneste har etter ekomforskriften § 6-2, jf. ekomloven § 2-8, plikt til å føre oversikt over enhver sluttbrukers navn, adresse og nummer/ adresse for tjenesten. Oversikten skal inneholde opplysninger som gjør det mulig å entydig identifisere de registrerte. Tilbyderen må dermed sørge for å legge til rette for hensiktsmessige rutiner for identifisering og autentisering av sluttbrukere. Dette gjelder særlig der salg av abonnement skjer via mellomledd (kiosker etc) eller via Internett. Kvaliteten på disse rutinene er grunnleggende for datakvaliteten i tilbyders oversikt over sluttbrukere. Dersom abonnementet knyttes til feil person vil følgelig all loggføring av senere trafikkdata være knyttet til feil person. Antakeligvis kan det ikke utledes noen plikt for tilbydere av Internettaksess til å identifisere sine abonnenter etter ekomloven § 2-8. Sett i lys av en eventuell implementering av EUs datalagringsdirektiv 2006/24/EF, og dets krav til tilbydere om lagring av ulike typer transaksjonsopplysinger, vil imidlertid dette spørsmålet om identifisering og datakvalitet bli aktualisert

[23] Modellen tar utgangspunkt i TCP/IP-referansemodellen for Internett og dens lagdeling av protokoller og tjenester. Av figuren kan man få inntrykk av at bruker og tjenesteyter kan kommunisere direkte med hverandre i tjenestelaget. I realiteten går all kommunikasjon gjennom kommunikasjonslaget. Ettersom visse spørsmål knyttet til identifisering og autentisering ikke løses av kommunikasjonslaget må disse løses på toppen av eksisterende infrastuktur og tjenester. Se nærmere om datanett-teori i Hannemyr, *Hva er internett*, Oslo 2005, s 57-64 og Tanenbaum, *Computer networks*, 4th, Upper Saddle River, N.J. 2003, s 37-48.

også i forhold til Internettabonnenter. Se nærmere om registreringsplikten i kapittel 4.1.

Tilbyder har som hovedregel taushetsplikt for lagrede trafikkdata og abonnementsopplysninger, men kan, dersom vilkårene for dette foreligger, utlevere slike opplysninger til politiet og påtalemyndigheten. Reglene om taushetsplikt for tilbyder, og andre som utfører arbeid eller tjeneste for tilbyder, følger av ekomforskriften kapittel 7, jf. ekomloven § 2-9. I utgangspunktet er det derfor bare tilbyder som vil ha kjennskap til koblingen mellom bestemte IP-adresser og den sluttbruker som har anvendt IP-adressen. Som vi skal se, har dette betydning for andre aktørers, f.eks. *tjenesteyteres*, mulighet til å anvende IP-adresser til å identifisere brukere av sine tjenester.

For å sikre at ikke uvedkommende får tilgang til brukerens maskin er det hensiktsmessig at maskinen er satt opp med et tilgangskontrollsystem (nr. 2 i figuren). Formålet med tilgangskontrollen vil ikke bare være å sikre at ikke uvedkommende kan tilegne seg de ressurser og tjenester som maskinen gir tilgang til, men også at ikke andre benytter maskinen til handlinger på Internett som brukeren kan risikere å bli konfrontert med, f.eks. handlinger som kan medføre straff eller erstatningsplikt. En særlig utfordring knytter seg til trådløse nettverk. Dersom brukeren ikke har satt opp tilfredsstillende sikkerhet på sitt trådløse nettverk vil andre, f.eks. naboer eller andre som befinner seg i nærheten, kunne knytte seg til nettverket og kommunisere på Internett ved hjelp av brukerens abonnement. Tilbyderen av elektronisk kommunikasjon vil normalt ikke kunne skille mellom abonnentens anvendelse av sitt abonnement og andres uautoriserte anvendelse. Alle loggførte transaksjonsopplysninger vil dermed i utgangspunktet assosieres med abonnenten. Dette vil kunne ha betydning for bevisbyrden dersom transaksjonsopplysninger lagret hos tilbyderen benyttes i en senere straffesak eller sivil tvist.

3.2.2 Relasjonen bruker – tjenesteyter (3) og (4)

I mange tilfeller vil det være viktig for brukeren å vite hvem han kommuniserer med over Internett. For eksempel vil det være viktig for brukeren å ha sikkerhet for at den websiden han har lastet ned faktisk tilhører nettbanken eller nettbutikken han ønsker å benytte seg av (nr 4 i figuren). Identifisering og autentisering av et nettsted og dets innehaver bygger på egenskaper ved kommunikasjonslaget, nærmere bestemt koblingen mellom virksomheten og et domenenavn (se nr 3 i figuren). Brukerens mulighet til å vurdere hvilket nettsted han har lastet ned avhenger av egenskaper ved brukerens nettleser, eventuelle sikkerhetstjenester som tilbys av webserveren og av hvordan sikkerhetstjenestene presenteres av nettleseren. Dersom brukeren er sikker på domenenavnet på det aktuelle nettstedet, vil en sjekk av nettstedets URL[24] i adressefeltet på nettleseren gi bekreftelse på at det er korrekt webside. Ytterligere sikkerhet kan oppnås ved bruk av serversertifikater[25] som krypterer kommunikasjonen mellom klient og server. Dette presenteres for brukeren ved at adressefeltet viser «https://». Enkelte nettlesere benytter i tillegg symboler, f.eks. hengelåssymbol i Internett Explorer, for å indikere at man er på en «sikker» webside med kryptert forbindelse. Et problem knyttet til standard serversertifikater er imidlertid at det tidligere har vært liten eller ingen kontroll med aktøren som har kjøpt tjenesten. Det har derfor ikke vært noe i veien for at serversertifikat har blir satt opp på «falske» nettsider hvor hensikten er å forlede brukeren med hensyn til hvem som faktisk står bak siden. Hvis brukeren da utelukkende bygger sin tillitt på adressefeltets visning av https eller hengelåssymbolet, men ikke sjekker den faktiske URL eller hvem som faktisk har fått sertifikatet utstedt til seg, vil brukeren kunne bli forledet til å utlevere opplysninger til et «utrygt» nettsted – riktignok med en «sikker» forbindelse.[26] Innføringen av EV (Extended Validation) SSL-sertifikater tar sikte på å endre denne situasjonen, hvor man som kjøper av et slikt sertifikat må gjennomgå en godkjenningsprosedyre som skal sikre at den som får et sertifikat utstedt til seg er den vedkommende hevder å være, og at nettstedet ikke blir brukt til ulovlig virksomhet.[27]

---

[24] URL er forkortelsen for Uniform Resource Locator.

[25] SSL (Secure Sockets Layer) og etterfølgeren TLS (Transport Layer Security) er krypteringsprotokoller basert på offentlig-nøkkel infrastruktur (PKI) som sikrer autentisering av server (men ikke klient), samt konfidensialitet og integritet for meldinger mellom klient og server.

[26] Selv om brukeren skulle ta seg tid til å sjekke hvem som står som sertifikatinnehaver, er det ikke sikkert at denne informasjonen er egnet til å gi brukeren noen holdepunkter for hvem som står bak nettstedet. Hvis f.eks. utvikling av nettstedet har vært delegert bort, har det forekommet at dette selskapets navn, og ikke oppdragsgivers navn, har blitt oppført som sertifikatinnehaver. Se nærmere om brukeropplevelsen av serversertifikater i Riisnæs, *Digitale sertifikater og sertifikattjenester - roller, oppgaver og ansvar*, Bergen 2007, kapittel 8.4.

3.2.3 Relasjonen tjenesteyter – bruker (5a) og (5b)

Vi har nå ryddet veien for å ta fatt på den relasjonen som har fått mest oppmerksomhet i personverndebatten, og hvor behovet for PETs blir aktualisert: virksomheters identifisering og autentisering av brukere (nr 5a og 5b i figuren). Ovenfor så vi at virksomhetens domenenavn (som korresponderer med en unik IP-adresse) ble benyttet for å autentisere webservere og bakenforliggende virksomhet. Brukeren vil imidlertid normalt ikke ha en unik IP-adresse som er egnet til å identifisere vedkommende overfor virksomheten, dessuten er kunnskap om koblingen mellom IP-adresse og bruker i utgangspunktet forbeholdt tilbyder av elektronisk kommunikasjon. Identifiseringav brukeren vil derfor hovedsakelig finne sted i det jeg har kalt *tjenestelaget* (nr 5a i figuren). Utfordringene her knytter seg blant annet til valg av hensiktsmessig identifikator (f.eks. brukernavn) og autentiseringsmekanisme (f.eks. passord). Se nærmere om dette i kapittel 3.3 under.

Proxyservere for å undertrykke IP-adresse

Selv om tjenesteyteren normalt vil måtte basere identifisering og autentisering av brukeren på tjenestelaget, er det enkelte personvernmessige utfordringer som knytter seg til kommunikasjonslaget (nr 5b i figuren). Her finner vi også en rekke tekniske tiltak (PETs) som *brukeren* kan ta initiativ til å anvende for å ivareta sitt personvern.[28] For eksempel vil brukerens IP-adresse være en potensiell mulighet for tjenesteytere til å generere en profil over nettbrukeres bruksmønster. Dette vil særlig kunne være et problem i tilfeller hvor brukeren har fast IP-adresse,[29] som gjør det mulig for tjenesteyteren å kjenne igjen IP-adressen fra sesjon til sesjon. Dersom brukeren ved en anledning blir identifisert (i tjenestelaget), vil tjenesteyteren i prinsippet kunne knytte denne informasjonen til IP-adressen for fremtidig bruk. Ved senere samhandling vil da brukeren anses som identifisert. Et teknisk tiltak for å avhjelpe disse personvernutfordringene knyttet til IP-adresser er bruk av anonymitets- eller pseudonymitetstjenester som undertrykker brukerens IP-adresse. Slike tjenester bygger på ruting av kommunikasjonen via flere proxyservere, slik at IP-adressen som formidles til tjenesteyter ikke er brukerens reelle adresse. Siden slike tjenester gjør det vanskelig å avdekke hvor den aktuelle server befinner seg, kan de også benyttes til (anonym) publisering som er motstandsdyktig mot sensur.[30]

Håndtering av informasjonskapsler

En annen personvernmessig utfordring som hører hjemme i kommunikasjonslaget er bruk av informasjonskapsler («cookies»). Protokollen for web, HTTP, er en statusløs protokoll som ikke holder rede på transaksjonshistorikken mellom nettleser og webserver. Dette er et problem ved f. eks. netthandel hvor det vil være en viktig funksjonalitet å sikre at websiden holder rede på hvilke varer kunden har valgt. Informasjonskapsler er en løsning på dette problemet og gjør det mulig for webserveren å lagre, og senere lese, små tekstfiler på brukerens maskin med blant annet statusinformasjon om den aktuelle eller tidligere sesjoner. Selv om informasjonskapsler slik sett er en nyttig teknologi, innebærer den også visse personvernmessige utfordringer. For eksempel gir informasjonskapsler tjenesteytere en potensiell mulighet til å kjenne igjen og danne profiler over brukeres nettbruk på tvers av sesjoner og nettsteder. Særlig gjelder dette for enkelte aktører, f.eks. leverandører av reklame eller søketjenester, som er representert på mange nettsteder og som kan følge nettbruken fra nettsted til nettsted. I likhet med IP-adresser vil en identifikasjon av brukeren i tjenestelaget i prinsippet gjøre det mulig å knytte identifiserende opplysninger til informasjonskapsler. Det finnes en rekke tekniske tiltak som kan gi brukeren kontroll over de personvernmessige implikasjonen ved informasjonskapsler. I tillegg til at standard nettlesere har funksjonalitet for å gi brukeren kontroll, finnes det software som brukeren kan velge å laste ned («cookie cutters» etc). Se nærmere om den rettslige reguleringen av informasjonskapsler i kapittel 4.1.

---

[27] EV SSL er utviklet av organisasjonen Certification Authority/Browser Forum (CAB Forum), se http://www.cabforum.org/. (sist nedlastet 25.01.2008). Utviklingen har skjedd i nært samarbeid med ledende nettleserprodusenter, som forventes å implementere løsningen blant annet ved bruk av fargekoder for å indikere sikkerhetsnivå nettsteder. Se omtale, Søiland, "Sikrere mot id-tyveri", *Computer World*, 15.01.2007, sist nedlastet 02.06.2008.

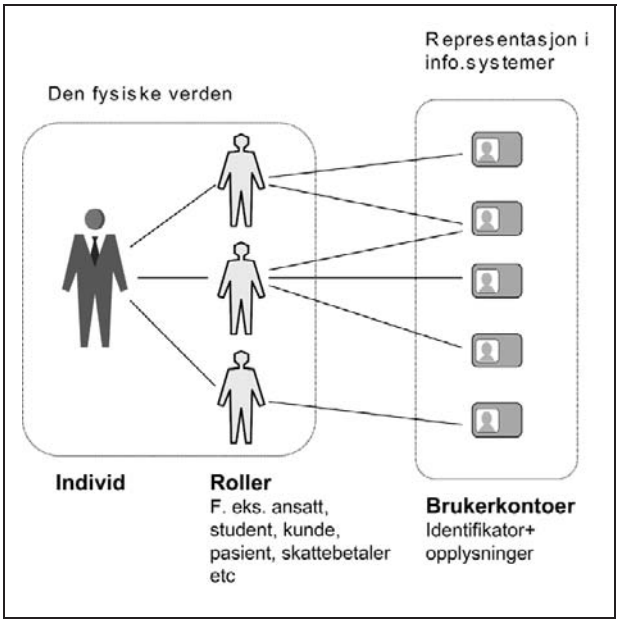
[28] Se f.eks. denne oversikten over "Privacy Tools" hos Electronic Privacy Information Center (EPIC), http://epic.org/privacy/tools.html

[29] I motsetning til dynamisk IP-adresse hvor brukeren tildeles en ny adresse for hver oppkobling til Internett.

[30] I dag er TOR-nettverket mest utbredt med flere hundretusen brukere internasjonalt, se http://www.torproject.org/. Se nærmere om slike tjenester i Øverlier, *Anonymity, privacy and hidden services*, Oslo 2007.

Støtte for informerte valg

I tillegg til tekniske løsninger for å undertrykke brukerens IP-adresse og kontrollere informasjonskapsler, har tekniske løsninger for å understøtte brukeren i å foreta informerte valg gjerne blitt omtalt som PETs. P3P (Platform for Privacy Preferences) er den tekniske løsningen som har fått desidert mest oppmerksomhet.[31] Formålet med P3P er å gjøre det enklere for brukeren å forstå nettsteders personvernpolicy, samt å legge til rette for automatiserte beslutninger basert på sammenlikninger mellom brukerens personvernpreferanser og nettstedets personvernpolicy. Dersom et nettsted samler inn personopplysninger vil personvernpolicyen være et naturlig sted å oppfylle personopplysningslovens krav til informasjon etter §§ 19 og 20. P3P gjør det mulig for virksomheten å uttrykke personvernpolicyen på tre nivåer: en kort og standardisert policy, en full policy og en maskinlesbar policy. Brukeren på sin side må benytte en nettleser som støtter P3P (f.eks. Internett Explorer), og stille inn nettleseren på ønsket personvernnivå før han kan surfe rundt på nettet. Så lenge de besøkte nettstedene har en P3P-personvernpolicy i overensstemmelse med brukerens angitte personvernnivå, vil brukeren ikke merke noe til P3P. Men dersom det ikke er match mellom brukers nivå og virksomhetens policy, vil brukeren bli gjort oppmerksom på det og få mulighet til å lese virksomhetens standardiserte policy i kort- eller fullt format. Mens det tidligere var stor entusiasme og forhåpninger knyttet til P3P, spesielt fra deler av IT-industrien, er det i dag en utbredt oppfatning om at P3P har sine begrensninger. Det er i hovedsak brukerrettede nettsteder tilknyttet store internasjonale selskaper som benytter teknologien, få brukere er kjent med den, og det er ingen garantier for at det som uttrykkes i slike policyer faktisk er korrekt eller overholdes i virksomheten.[32] P3P har i dag størst praktisk betydning i forhold til å automatisk godkjenne eller hindre lagring av informasjonskapsler.[33]



Figur: 4.3 Individ, roller og brukerkontoer

3.3 Nærmere om «identitet» og identitetsforvaltning

Som avsnittet over viser dukker spørsmålet om identitet og identitetsforvaltning opp i flere relasjoner. Her skal vi se nærmere på relasjonen mellom brukeren og tjenesteyteren (5a) i figuren. Problemstillingen videre er hva som menes med «identitet». Videre skal vi se nærmere på hvordan tjenesteyteren kan få etablert tilstrekkelig sannsynlighet for at en påstand om identitet er riktig.

Identitet er et sammensatt og komplekst begrep. I forhold til elektronisk samhandling kan det være nyttig å sondre mellom individet og individets ulike roller i den fysiske verden, og representasjon av slike roller i form av brukerkontoer i informasjonssystemer. Se figur 4.3.

For så vidt kan begrepet «identitet» benyttes om alle de tre nivåene (individ, roller og brukerkontoer) i figur 4.3. I tilegg kan begrepet benyttes både om selve brukerkontoen og om identifikatoren (f.eks. brukernavnet) som skiller brukerens brukerkonto fra andre brukerkontoer. For å unngå misforståelser er det derfor viktig å presisere

[31] Se http://www.w3.org/P3P/

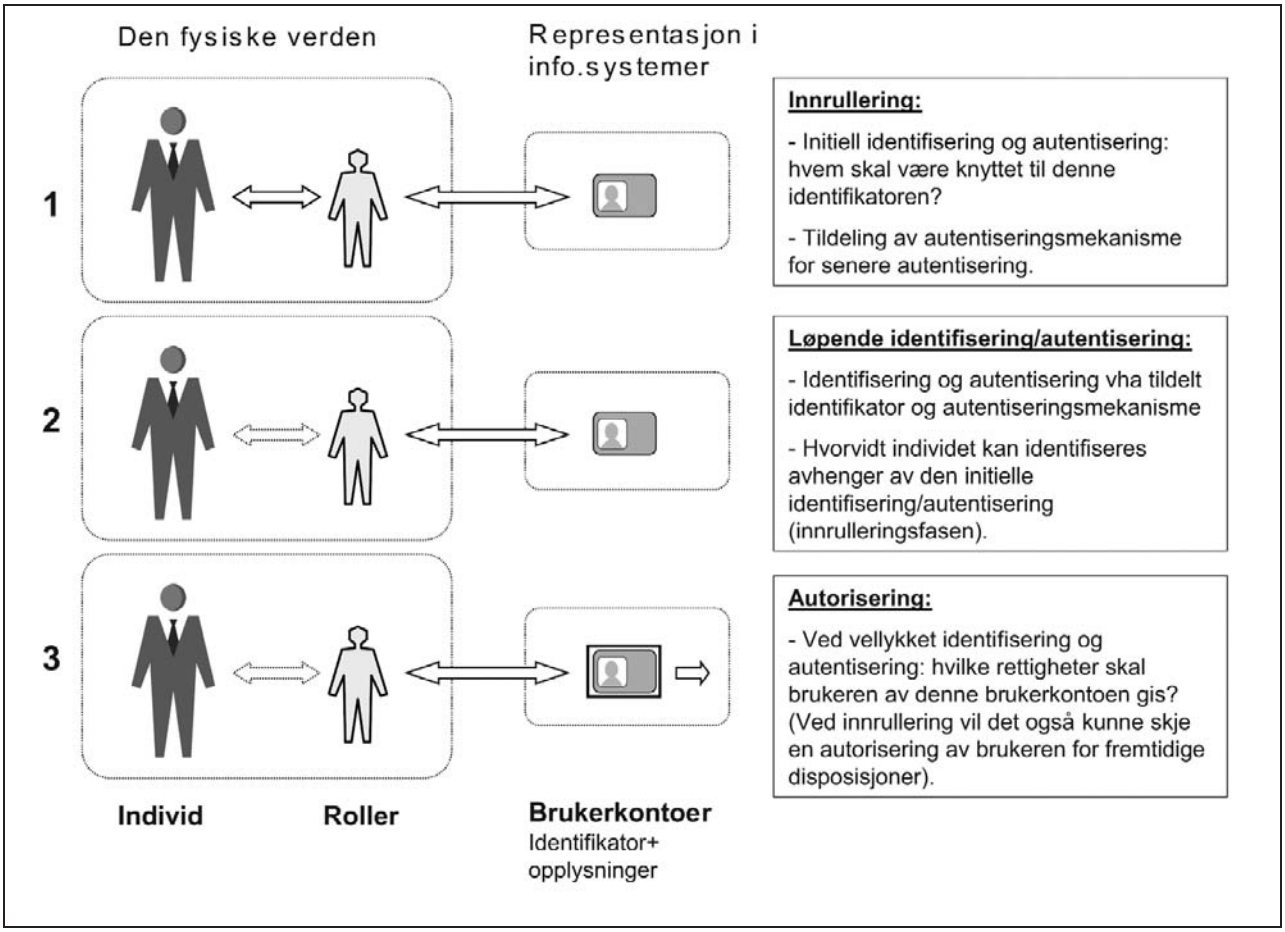
[32] Det skal nevnes at det også er blitt forsket på tekniske løsninger som gjør det mulig å angi detaljerte regler for hvordan *lagrede* personopplysninger skal behandles. IBM har f.eks. utviklet EPAL (Enterprise Privacy Authorisation Language) som bygger på forutsetningen om at alle personopplysninger i en virksomhet tagges med metadata, og det angis regler for hvem, som for hvilket formål og under hvilke forutsetninger, kan behandle opplysningene. Tilnærmingen har en viss sammenheng med P3P. Begge bygger på bruk av XML-baserte regelsett, og man har sett for seg at det som uttrykkes utad om virksomhetens behandling av personopplysninger gjennom P3P kan håndheves internt gjennom EPAL. Se http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/.

[33] Her kan det sondres mellom informasjonskapsler som faktisk er fra nettstedet man besøker, informasjonskapsler fra tredjeparter (f.eks. fra reklamebannere) og informasjonskapsler fra sider som benytter/ikke benytter P3P.

hva man mener med identitet. Dette gjelder ikke minst i spørsmål knyttet til såkalt «identitetstyveri».

Erkjennelsen av at man som samfunnsborger daglig veksler mellom ulike roller er viktig for å kunne legge til rette for tekniske løsninger som er hensiktsmessige og forsvarlige fra et personvernsynspunkt. For eksempel vil det kunne være stor forskjell på hvilke opplysninger som vil være relevante og som det vil være ønskelig å dele med familie, venner, lærested, arbeidsgiver, helsevesen, forsikringsselskap, skattevesen eller Internett- og telefonleverandør. Utviklingen i retningen av økt elektronisk samhandling skaper utfordringer i forhold til å tilpasse identifisering og autentisering til den aktuelle rolle og relasjon.

> «Et eksempel er dagens bruk av e-post. For mange arbeidstakere og studenter utgjør e-postadressen de har fått tildelt av arbeidsgiver eller lærested en viktig kommunikasjonskanal. Det er blitt vanlig å benytte denne e-postadressen ikke bare i forhold til jobb eller studier, men også til fortrolig kommunikasjon med familie og venner, og gjerne også offentlig etater og kommersielle aktører. E-postadressen, som i utgangspunktet er ment å bli brukt til jobbrelatert kommunikasjon, blir på denne måten også benyttet i mange sammenhenger hvor rollen som ansatt eller student er helt uvesentlig, men hvor det er vedkommendes rolle som familiemedlem, venn, borger eller kunde som er det sentrale. Det er nok flere grunner til at mange velger å benytte e-postadressen til mange formål som ikke er relatert til vedkommendes arbeidsoppgaver. For det første kan det gjerne oppleves som tungvint å benytte flere e-postadresser da dette med normalt medfører at man må holde seg à jour med flere e-postadresser. For det andre har det i mange tilfeller ikke vært noe i veien for å benytte e-postadressen til annet enn jobb/studierelatert kommunikasjon. Samtidig har skillet mellom arbeid og fritid gradvis blitt visket ut – noe som også kan forklare hvorfor jobbrelatert e-postadresser også blir benyttet til andre formål. Spørsmålet om arbeidsgivers innsynsrett i arbeidstakers e-post har av Datatilsynet, domstolene og lovgiver tatt utgangspunkt i skillet mellom privat e-post (som arbeidsgiver i utgangspunktet ikke har hatt innsynrett i), og virksomhetsrelatert e-post (hvor utgangspunktet har vært rett til innsyn). Skillet mellom privat og virksomhetsrela-



Figur: 4.4 Faser

tert har i praksis vist seg å være vanskelig å trekke opp. Hadde det vært lagt bedre til rette for at arbeidstakere enkelt kunne bytte fra en rolle til en annen ville antakelig denne problemstillingen ikke vært like aktuell. Det kunne da stilles krav til at arbeidstakere benyttet denne muligheten, noe som ville sikre at det allerede ved utsendelse og mottak av e-post ble skilt mellom jobbrelatert og annen «privat» kommunikasjon. Et eventuelt innsyn av arbeidsgiver ville da være med utgangspunkt i det som allerede fremstår som virksomhetsrelatert e-post. Dette ville i så fall være vesentligere enklere og mer personvernvennlig enn det som har vært tilfellet tidligere: gjennomgang og sortering av all e-post.»

I det følgende skal vi se nærmere på identitetsforvaltningens grunnleggende faser. Som vi skal se, avhenger de personvernmessige aspektene særlig av valg av identifikator og autentiseringsmekanisme.

3.4 Sentrale faser

Identitetsforvaltning kan, som illustrert i figur 4.4, brytes opp i tre grunnleggende faser: innrullering, løpende autentisering og autorisering.

Nærmere om de enkelte fasene:

(1) Innrullering

I innrulleringsfasen er det gjerne fire spørsmål som må adresseres:

- Med hvilken grad av sikkerhet trenger man å vite *hvem* som innrulleres?
  Trenger man å vite hvem brukeren er? Hvis ja, hvordan etablere tilstrekkelig sikkerhet for at brukeren er den han hevder å være (autentisering)?
- Hvilken *identifikator* skal være knyttet til denne brukeren? (f.eks. brukernavn)
- Hva slags *autentiseringsmekanisme* skal brukeren utstyres med? (f.eks. passord)
- Hva skal denne brukeren eventuelt være *autorisert* til å foreta seg i systemet?

(2) Løpende identifisering og autentisering

Når brukeren vender tilbake for å benytte tjenesten, må det skilles mellom to prosesser:

- Identifisering: brukeren individualiseres fra andre lagrede brukere på bakgrunn av identifikatoren som oppgis (f.eks. brukernavn)
- Autentisering: brukeren benytter autentiseringsmekanismen som bekrefter at han/hun er den som fikk utdelt identifikatoren.

Merk at resultatet av disse to prosessene ikke nødvendigvis medfører at systemet har avdekket *hvem* brukeren er (i betydningen personens alminnelige brukte navn eller identifikator). Hva man vet om brukeren etter vellykket identifisering og autentisering avhenger av innrulleringsfasen og kvaliteten på identifiserings og autentiseringsprosessene der. Dersom det ikke ble foretatt noen autentisering av brukeren i innrulleringsfasen, vil resultatet her simpelthen være at man har en viss grad av sikkerhet for at det er den samme brukeren som nå har logget inn.

(3) Autorisering

Dersom den løpende identifiseringen og autentiseringen er vellykket er spørsmålet hvilke ressurser og tjenester brukeren skal ha tilgang til (autorisering).

3.5 Nærmere om autentisering

I gjennomgangen av fasene over kan man få inntrykk at autentisering bare knytter seg til å etablere tilstrekkelig sikkerhet for en påstått identitet. Det er imidlertid også andre forhold det kan være viktig å etablere sikkerhet om. I mange tilfeller er ikke nødvendigvis identitet så interessant i forhold avgjørelser om å gi eller nekte tilgang til en tjeneste eller ressurs. Man kan skille mellom autentisering av:

- Identitet (I betydningen personidentifiserende opplysninger som f.eks. navn, adresse og fødselsnummer)
- Rolle (Man trenger ikke nødvendigvis vite hvem personen er, så lenge man kan få bekreftet at vedkommende innehar en relevant rolle som f.eks. student, ansatt eller kunde)
- Attributt (Egenskaper som alder, kjønn, betalingsevne og -vilje etc)

Ved tradisjonelle kommunikasjonsformer vil det ofte være mulig å fysisk observere den identitet, rolle eller egenskap som påberopes. Hvis en godt voksen person ønsker å kjøpe kinobillett til en forstilling med 7-årsgrense, ville det vekke oppsikt om kassadamen ba om ID-kort for å sjekke personens alder. Dersom hun mot formodning skulle be om ID-kort, ville autentiseringen bygge på følgende premisser: Er dette et ID-kort som ser ekte ut og som er utdelt etter en tilfredsstillende identitetsautentisering? Er personen den samme som er avbildet på kortet? Normalt vil kontantbetalingen også godtas også uten forespørsel om *hvem* personen er. I dette tilfellet kan kassadamen fysisk observere alder og kontanter – egenskapene

er det man kan kalle *selvautentiserende*.[34] Videre vil det normalt ikke være behov for å lagre personidentifiserende opplysninger.

Ved elektronisk kommunikasjon er utgangspunktet at vi ikke kan basere oss på slik selvautentisering hvor egenskaper kan sanses eller observeres. Opplysninger som kan underbygge påstanden må da kommuniseres av den enkelte, eller av andre som har tilgang til slike opplysninger. Dersom billetten kjøpes på nettet ville det normale forløpet være at personens identitet blir kjent i forbindelse med gjennomføring av betalingen. Videre vil opplysinger om brukerens kjøp kunne bli lagret både hos kortselskap og billettselger.

Eksemplet overfor viser at den samme transaksjonen vil arte seg forskjellig avhengig av om den foretas ved fysisk nærvær eller over Internett. Videre skal vi kort se nærmere på *hvordan* man autentiserer ved elektronisk samhandling. Det skjelnes gjerne mellom fire ulike mekanismer for autentisering, nemlig noe man:

- *er* (biometriske kjennetegn),
- *vet* (f.eks. passord)
- *har* (f.eks. smartkort, kortleser, informasjonskapsel, mobilnummer eller postforsendelse til folkeregistrert adresse)
- *gjør* (f.eks. karakteristika som trykk, hastighet og bevegelsesmønster når man påfører en signatur)

Enkelte av autentiseringsmekanismene, f.eks. biometri, reiser nye personvernspørsmål som det ikke er anledning til å ta opp her. Budskapet i denne sammenheng er at man fra et personvernsynspunkt bør gå vekk fra betraktningen om at identifisering handler om å avdekke den enkeltes «sanne» identitet. I enkelte tilfeller er identitet irrelevant, i stedet bør det legges til rette for å autentisere den rolle eller egenskap som er av interesse.[35]

3.6 Systemer og standarder for identitetsforvaltning

Utviklingen i retning av stadig mer elektronisk samhandling med et økende antall relasjoner, medfører et behov for systemer og løsninger for identitetsforvaltning.

Fra den enkelte *brukers perspektiv* handler identitetsforvaltning om håndtering av ulike «brukerkontoer». Rent praktisk vil det si håndtering av et økende antall korresponderende identifikatorer og autentiseringsmekanismer (passord, smartkort, digitale sertifikater etc). Fra brukerens synspunkt kan dette oppleves som en stadig større utfordring, noe som kan føre til at enkelte skriver ned passordene eller velger det samme passordet flere steder. Fra et sikkerhets- og personvernperspektiv er dette uheldig. En brukerstyrt teknisk løsning på denne utfordringen er f.eks. å finne i standard nettlesere hvor brukeren kan velge å bli assistert i å knytte brukernavn og passord til rett nettsted.

Fra *virksomheters perspektiv* dreier identitetsforvaltning seg om tildeling og vedlikehold av brukerkontoer. Dette inkluderer, som nevnt i kapittel 3.4, innrullering, løpende identifisering/autentisering og autorisering av brukere. Tradisjonelt har dette vært løst av virksomhetene selv, gjerne med én særegen løsning for hvert system. Mange virksomheter har erfart at det kan være en ressurskrevende oppgave å drifte mange systemer med ulike påloggingsløsninger. Dette kan medføre dårlig oversikt over eksisterende brukerkontoer, og brukerne må forholde seg til mange brukernavn og passord. Identitetsforvaltning handler derfor om hvordan man kan effektivisere de aktuelle arbeidsprosessene, blant annet ved å legge til rette for felles tilgangssystemer (single sign-on) hvor én innlogging gir tilgang til flere systemer og tjenester. Med utgangspunkt i åpne tekniske standarder er det nå mulig å implementere identitetsforvaltningsløsninger som ikke bare gjelder virksomhetens egne ansatte, men som også omfatter kunder og samarbeidspartnere. Nye e-forvaltningsløsninger som MinSide er et eksempel på dette, der én enkelt autentisering gir tilgang til nett-tjenestene til flere uavhengige statlige og kommunale etater.

Nye identitetsforvaltningsløsninger gir altså muligheter for nye forretningsmodeller og e-forvaltningsløsninger ved at sentrale arbeidsprosesser knyttet til innrullering og løpende identifisering/autentisering kan foretas av spesialiserte identitetsforvaltere. Hva brukeren skal få tilgang til (autorisering), blir som oftest besluttet lokalt etter en vellykket autentisering av en ekstern identitetstilbyder (f.eks. BankID). I utgangspunktet må det forventes at personvernet og informasjonssikkerheten blir bedre ivaretatt når profesjo-

[34] Se Lessig, *Code: version 2.0*, New York 2006, s 40.

[35] Et interessant eksempel er eBay og enkelte andre e-handelsplatformer som har hatt suksess med omdømmesystemer for å formidle informasjon om selgere og kjøpere. I slike systemer er det aktørenes opparbeidede omdømme som er det sentrale, ikke identitet. Se nærmere Mahler og Olsen, "Reputation Systems and Data Protection Law", I: *eAdoption and the Knowledge Economy: Issues, Applications, Case Studies*, Cunningham og Cunningham (red), 2004.

nelle identitetforvaltere tar hånd om deler av identitetsforvaltningen, enn om f.eks. hver enkelt statlige og kommunale etat skulle drifte sine egne løsninger. Det er også opplagt at felles tilgangsløsninger som MinSide gjør det mulig å tilby samfunnsnyttige tjenester, men også tjenester som direkte kan gavne personvernet, f.eks. ved å gi innsyn i hvilke opplysninger de enkelte etatene har om den enkelte borger. Det skal imidlertid ikke legges skjul på at utviklingen reiser prinsipielle personvernspørsmål. Tradisjonelt har virksomhetsgrenser vært en av de viktigste barrierene for ivaretakelse av personvernet: ved å holde relasjoner og kontekster atskilt har man kunnet unngå enkeltaktører som «vet alt» om den enkelte borger. Spissformulert kan man si det slik at løsninger for identitetsforvaltning tar sikte på å bryte ned slike barrierer og gjøre opplysninger tilgjengelige på tvers av system- og virksomhetsgrenser. Riktignok tar løsningene gjerne utgangspunkt i at det bare er brukeren selv som skal ha fordelen av å kunne få enkel tilgang til de ulike tjenester, og at opplysningene fremdeles skal være lagret hos den enkelte virksomhet. Dette er imidlertid ingen garanti for at løsningene ikke vil kunne være sårbare for misbruk og legge til rette for utveksling av personopplysninger som ellers ikke ville blitt utvekslet.[36] Et annet aspekt som bør synliggjøres er at identitetsforvaltningsløsninger tar sikte på å tilby en sømløs og brukervennlig brukeropplevelse på tvers av virksomhetsgrenser. Dette hensynet kan i noen tilfeller komme i konflikt med personvernhensyn, hvor prinsippet om brukermedvirkning og kontroll tilsier at brukeren skal være i stand til å vurdere implikasjonene ved å benytte en tjeneste. Dette fordrer at aktørene er sine roller og oppgaver bevisst og at informasjon om disse forhold formidles til brukeren på en hensiktsmessig måte.[37]

4 Personopplysningslovgivningen

Fremstillingen har så langt gitt en oversikt over de personvernmessige aspektene knyttet til personvernøkende teknologi og identitetsforvaltning. Når fokuset nå rettes over på det rettslige vernet om personopplysninger er hensikten å kortfattet synliggjøre enkelte sammenhenger mellom jus og teknologi. Dette gjelder for det første i hvilken grad personopplysningslovgivningen stiller krav til teknologien (kapittel 4.1). For det andre forholdet mellom enkelte av personopplysningsrettens grunnleggende prinsipper og PETs/identitetsforvaltning (kapittel 4.2).

4.1 Hva reguleres?

Personopplysningsloven (pol) er den sentrale loven på området. Loven gjennomfører Norges forpliktelser etter personverndirektivet 95/46/EF og gjelder for «behandling av personopplysninger». Dette betyr at loven kun gjelder i den grad opplysninger kan knyttes til en identifiserbar enkeltperson. Loven retter seg mot den «behandlingsansvarlige», det vil si den som bestemmer formål og virkemidler for behandlingen. Den behandlingsansvarlige må således følge visse materielle og prosessuelle krav for at behandlingen skal være lovlig.

Personopplysningsloven stiller i utgangspunktet ikke direkte krav til teknologien. Det som reguleres er den behandlingsansvarliges behandling av personopplysninger. Loven sier altså ikke noe direkte om hvordan ny teknologi skal utvikles eller hvordan tekniske standarder skal utformes. Det er først når teknologien *anvendes* av en behandlingsansvarlig for å behandle personopplysninger at de rettslige kravene gjør seg gjeldende. I utgangspunktet gir det derfor ikke mening å snakke om «godkjente» produkter, systemer eller standarder. Ikke overraskende vil det være lettere å overholde personopplysningslovgivningen dersom man har tatt hensyn til personverninteresser og lovens krav ved utvikling av teknologien. Det

[36] Et eksempel på en kommersiell løsning som hadde åpenbare personvernsvakheter var Microsoft .NET Passport. Tjenesten tok utgangspunkt i Microsoft sin Hotmail-tjeneste (e-post), hvor innlogging her gav anledning til single sign-on hos f.eks. eBay og andre store kommersielle aktører. Etter kritikk fra Artikkel 29-arbeidsgruppen (rådgivende arbeidsgruppe bestående av representanter fra datatilsynsmyndighetene i EU-landene), endret Microsoft i 2003 tjenesten til kun å gjelde egne tjenester. I tillegg til kritikk for selve implementasjonen (måten samtykke ble innhentet på, manglende informasjon, uklare ansvarsforhold etc) var arbeidsgruppen kritisk til den tekniske arkitekturen som innebar Microsoft selv som eneste identitetsforvalter, samt bruk av en unik identifikator for hver bruker. Arkitekturen var sårbar for misbruk siden Microsoft satt på mye informasjon om bruken av tjenesten, og hvor kun avtalemessige forhold hindret tjenesteyterne fra å samkjøre informasjon om felles kunder. Se nærmere om dette i Olsen og Mahler, "Identity management and data protection law: Risk, responsibility and compliance in `Circles of Trust'", *Computer Law & Security Report*, 4 & 5, 2007 342-351 & 415-426.

[37] Se nærmere om roller og oppgaver og om oppfyllelse av informasjonsplikten etter personopplysingslovgivningen i Olsen og Mahler, "Identity management and data protection law: Risk, responsibility and compliance in `Circles of Trust'", *Computer Law & Security Report*, 4 & 5, 2007 342-351 & 415-426 og Olsen og Mahler, *Identity management & Privacy*, Complex, 2007.

avgjørende i følge loven er imidlertid hvordan teknologien implementeres og anvendes av den behandlingsansvarlige. Dersom den behandlingsansvarlige velger å sette bort hele eller deler av behandlingen til en databehandler, er lovens system at det fremdeles er den behandlingsansvarlige som har ansvaret for at lovens regler følges. Det er grunn til å tro at det hersker en utbredt misoppfatning om at man kan overholde personopplysingsloven ved å kjøpe en fiks ferdig teknisk løsning, eller ved å delegere bort behandlingen til en profesjonell aktør. Gode tekniske løsninger og kompetente samarbeidspartnere er vel og bra, men den behandlingsansvarlige sitter altså fremdeles med hovedansvaret.

I forhold til temaet personvernøkende teknologi og identitetsforvaltning er det også relevant å rette oppmerksomheten mot enkelte bestemmelser i lov og forskrift om elektronisk kommunikasjon (ekomloven og -forskriften). Bestemmelsene retter seg primært mot tilbyder av elektronisk kommunikasjonsnett eller -tjeneste, det vil si aktører som enten gir tilgang til elektronisk kommunikasjon (herunder telefonitjenester og Internett), eller som overfører signaler for slike tjenester. Som nevnt i kapittel 3.2 har tilbydere av offentlig telefontjeneste plikt etter ekomforskriften § 6-2, jf. ekomloven § 2-8, til å føre oversikt over enhver sluttbrukers navn, adresse og nummer/adresse for tjenesten. Oversikten skal inneholde opplysninger som gjør det mulig å entydig identifisere de registrerte. Selv om lov og forskrift ikke sier det direkte, må det antas at det implisitt i registreringsplikten er et krav om autentisering av sluttbrukeres identitet ved tegning av abonnement. Hvis ikke vil abonnentopplysningene riktignok kunne entydig identifisere den registrerte, men man vil ikke ha noen sikkerhet for at det er rett person. I praksis har det vist seg at tilbyderne av elektronisk kommunikasjon har hatt problemer med å oppfylle registreringsplikten på en tilfredsstillende måte.[38] Dette kan for det første skyldes ønsket om å gjøre tegning av abonnement så enkelt som mulig, f.eks. over Internett eller i kiosken på hjørnet. For det andre skyldes det en lav kollektiv bevissthet om skillet mellom identifisering og autentisering. Fødselsnummer er en personentydig identifikator som er godt egnet til identifisering ved at den individualiserer ett individ fra alle de andre. Fødselsnummer skal imidlertid ikke benyttes til autentisering. Fødselsnummeret er nemlig ingen hemmelighet som gir sikkerhet for at den aktuelle personen er den han hevder å være. Dersom man har anledning til å benytte fødselsnummer som identifikator, jf. pol § 12, må det derfor i tillegg benyttes en eller flere autentiseringsmekanismer som gir sikkerhet for at et fødselsnummer faktisk er knyttet til den aktuelle personen, jf. kapittel 3.5 over.

Ekomloven med forskrift innholder også andre viktige bestemmelser om vern av personopplysninger. Dette gjelder blant annet regler om taushetsplikt og om behandling av trafikk- og lokasjonsdata. Som nevnt i kapittel 3.2 har det i personvernkretser vært mye fokus på informasjonskapsler og de muligheter denne teknologien gir til å samle informasjon om internettbrukere på tvers av nettsteder og sesjoner. Faktisk er informasjonskapsler regulert i ekomforskriften § 7-3, hvor utgangspunktet er at det er *forbudt* å benytte informasjonskapsler «uten at bruker er gitt informasjon av den behandlingsansvarlige i henhold til personopplysningsloven, herunder om behandlingsformålet og er gitt anledning til å motsette seg behandlingen.» Forbudet gjelder likevel ikke dersom det gjelder «teknisk lagring» utelukkende for det formål å overføre eller lette overføringen, eller dersom slik lagring eller adgang til opplysninger er «nødvendig for å levere en informasjonssamfunnstjeneste etter brukerens uttrykkelige forespørsel». Bestemmelsen er oppsiktsvekkende. Den retter seg for det første ikke primært mot *tilbydere* slik loven og forskriften ellers gjør, men mot «*tjenesteytere*» som benytter informasjonskapsler (jf. skillet mellom ISP og tjenesteytere i figur 4.2). For det andre er det et forsøk på rettslig regulering av et spørsmål av svært praktisk karakter hvor gjennomføringen av informasjonsplikten nødvendigvis må skje gjennom tekniske tiltak. I praksis er nok denne bestemmelsen relativt ukjent for pliktsubjektene, og brukerne må sies å være best stilt ved å stole på de tekniske hjelpemidler de har til rådighet for å kontrollere lagring og lesning av informasjonskapsler, jf. kapittel 3.2. Bestemmelsen står dessuten i sterk kontrast til personvernregelverket ellers, som gjennomgående er teknologinøytralt. Generelt kan det sies at personvernbestemmelsene i ekomloven og ekomforskriften er viktige, men at de er godt gjemt i et regelverk som primært angir konkurranseregler innenfor elektronisk kommunikasjon.

[38] Sommeren 2007 ble f.eks. nett-tjenesten til Tele2 benyttet til å hente ned fødselsnummer, navn , adresse og kredittverdighet for 60 tusen personer. Se omtale i Hannemyr, "Feil nummerbruk", *Lov&Data*, 92, 2007 29-30. Se også Olsen, "Lovgivningsprosessen bak registreringsplikt for kontantkort til mobiltelefon", *Lov & Data*, 85, 2006 1-6.

4.2 Grunnleggende personvernprinsipper

Personvernopplysningsretten kan uttrykkes gjennom noen grunnleggende prinsipper som gjelder for all behandling av personopplysninger. De grunnleggende prinsippene kan sies å være selve kjernen i internasjonal og nasjonal personvernregulering. Hvert prinsipp representerer således et sett med mer detaljerte regler som skal ivareta et nærmere bestemt hensyn eller en regulatorisk strategi som anses hensiktsmessig for å ivareta personvernet i forbindelse med behandling av personopplysninger. Prinsippene kan skisseres på følgende måte:

Rettmessig og rettferdig behandling:

All behandling av personopplysninger krever rettslig grunnlag, og den behandlingsansvarlige skal ta tilbørlig hensyn til den registrertes berettigede personverninteresser. Sensitive personopplysninger er underlagt strengere vern enn alminnelige personopplysninger.

Brukermedvirkning og kontroll:

Den behandlingsansvarlige skal gjøre behandlingen transparent og forståelig for den registrerte, slik at denne gjøres i stand til å overskue behandlingens konsekvenser og er i stand til å ivareta sine personverninteresser.

Formålsbestemthet:

Den behandlingsansvarlige skal før innsamling og behandling av personopplysninger angi et klart og uttrykkelig formål med behandlingen. Opplysningene skal ikke senere benyttes for uforenlige formål.

Minimalitet:

Personopplysninger bare skal innhentes, lagres og behandles i den grad de er nødvendige for å oppnå formålet med behandlingen av opplysningene.

Datakvalitet:

Personopplysninger skal ha tilstrekkelig kvalitet i forhold til det formålet de skal anvendes til. Dette innebærer blant annet at opplysningene skal være tilstrekkelig oppdaterte, presise og relevante sett opp mot formålet med behandlingen.

Informasjonssikkerhet:

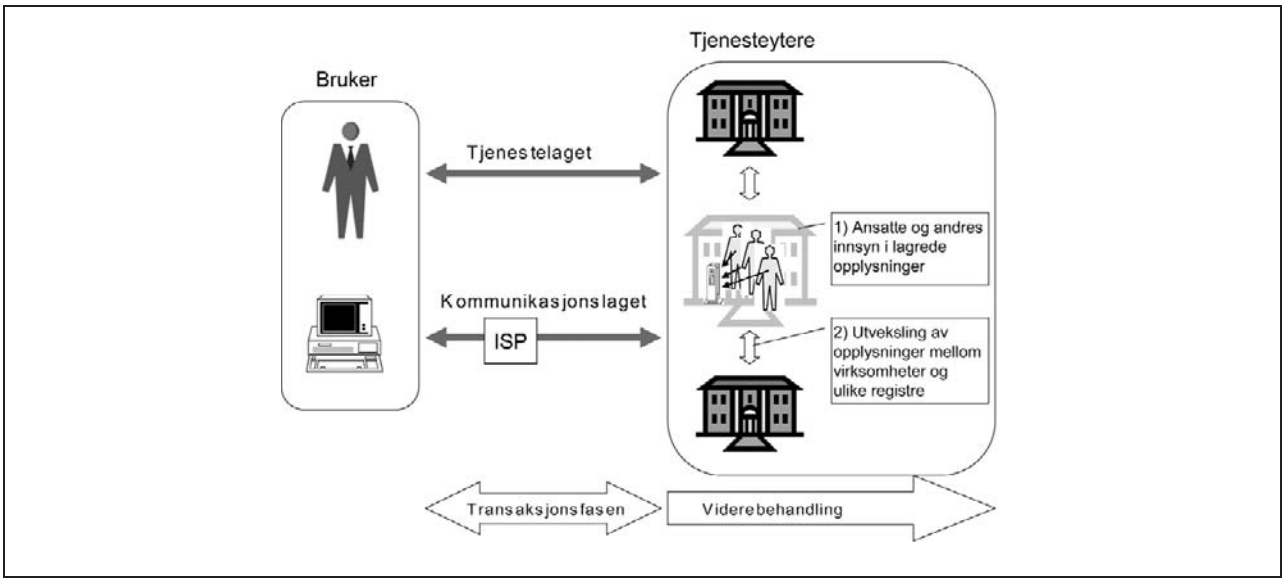
Den behandlingsansvarlige (og databehandleren) skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

De personvernutfordringene PETs og identitetsforvaltning (se kapittel 2 og 3) tar sikte på å løse eller avhjelpe, kan i og for seg knyttes til alle disse prinsippene. Etter min oppfatning er det imidlertid særlig grunn til å se nærmere sammenhengen mellom PETs/identitetsforvaltning og prinsippene brukermedvirkning og kontroll, minimalitet og datakvalitet.

4.2.1 Brukermedvirkning og kontroll

Prinsippet om brukermedvirkning og kontroll kommer til uttrykk i personvernlovgivningens bestemmelser som skal sikre transparens, det vil si bestemmelser om samtykke som behandlingsgrunnlag, informasjonsplikt, innsynsrett og meldeplikt. Gjennomgangen av P3P viser at det finnes tekniske løsninger for å støtte opp under formidlingen av såkalte personvernpolicyer. Videre har vi sett at autentiserings- og identitetsforvaltningsløsninger gjør det mulig å gjennomføre innsynsretten på en mer effektiv måte. Brukermedvirkning og kontroll handler også om at brukeren skal kunne ha kontroll på utlevering og videre behandling av egne personopplysninger. Et grunnleggende skille er derfor mellom «transaksjonsfasen» hvor brukeren kan velge å utlevere opplysninger, og «videre behandling» hvor opplysninger om brukeren er blitt utlevert. Når opplysninger først er blitt utlevert har brukeren liten eller ingen kontroll på behandlingen. Fra et personvernsynspunkt er det da særlig to spørsmål som gjør seg gjeldende: (1) hvem i virksomheten skal ha tilgang til opplysningene; og (2) i hvilken grad kan opplysninger utveksles mellom virksomheter og ulike registre. Skillet mellom transaksjonsfasen og videre behandling illustreres i figur 4.5.

Som vi så av gjennomgangen i kapittel 3.2, kan det være hensiktsmessig å skille mellom identitetsforvaltning i kommunikasjons- og tjenestelaget. Begge disse lagene knytter seg til transaksjonsfasen i figuren. Som nevnt har de klassiske PETs tatt sikte på å gi brukeren kontroll over potensielt identifiserende opplysninger i kommunikasjonslaget (f.eks. proxyservere eller «cookiecutters» for å undertrykke IP-adresse eller informasjonskapsler).



Figur: 4.5 Transaksjonsfase og videre behandling

4.2.2 Prinsippene minimalitet og datakvalitet

Som vi har sett har PETs tradisjonelt vært sett på som tekniske og organisatoriske tiltak som tar sikte på å kontrollere adgangen til å identifisere den opplysningene gjelder. Også på det rettslige og politiske planet er minimalitet og anonymitet viet stor oppmerksomhet – dog med litt forskjellige innfallsvinkler. Viktigheten av anonymitet fremkommer for det første av en rekke internasjonale rekommandasjoner angående Internett og autentiseringsløsninger.[39] Her hjemme har spørsmålet om anonymitet særlig blitt synliggjort av Datatilsynet som i tilknytning til bompengeringene har fremhevet viktigheten av å kunne *ferdes* anonymt. I personvernteori legges av og til prinsippet til grunn for en *rett* til anonymitet eller et eget *prinsipp* om anonymitet.[40] Også i regjeringens IKT-politikk fremheves «at det fremdeles må være tilbud om anonyme løsninger i sammenhenger der det ikke er nødvendig å identifisere seg.»[41]

Gjeldende lovgivning står imidlertid etter min mening i en klar kontrast til de nevnte uttalelsene om viktigheten av anonymitet. Prinsippet kan skimtes i personopplysningsloven § 11 d) som stiller krav til at opplysninger er «tilstrekkelige og relevante«[42] for formålet med behandlingen, og § 11 e) om at opplysningene ikke skal lagres lenger enn det som er nødvendig ut fra formålet med behandlingen. Videre kan man kanskje innfortolke et krav om å begrense innsamling av opplysninger i «nødvendighetsvilkårene» i §§ 8 og 9 ut fra synspunktet om at dersom formålet kunne vært oppnådd uten identifiserbare data så er behandlingen av opplysningene ikke nødvendig.[43] Konklusjonen må uansett være at personopplysningsloven i liten grad setter krav til eller legger føringer for minimalitet og anonymitet. Kort oppsummert oppstiller loven et forbud mot å samle inn irrelevante opplysninger, og en plikt til å slette eller anonymisere opplysninger når formålet er oppnådd. Loven legger altså ingen føringer for anonymitet eller pseudonymitet i det jeg i Figur 5 har kalt «transaksjonsfasen». Det er, som vi har sett i avsnittet over, i denne fasen brukeren har en reell mulighet til å ha kontroll på egne opplysninger. Når identifiserende opplysninger først er samlet inn (videre behandling) har brukeren liten eller ingen kontroll.

I forbindelse med revisjon av personopplysningsloven er det blitt fremmet forslag om unntak

[39] Se f.eks. Artikkel 29-gruppens rekommendasjoner om anonymitet på Internett (WP 6/1997) og autentiseringstjenester (WP 68/2001).

[40] Se f.eks. Schartum og Bygrave, *Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger*, Bergen 2004, s 93-94.

[41] Se St.meld. nr 17 (2006-2007), kapittel 8.3.3 ”Retten til å være anonym”.

[42] I direktivet er dette formulert som ”relevante og ikke for omfattende”. Minimalitetsprinsippet er altså noe tydeligere i direktivet, mens personopplysningsloven synes altså å vektlegge tilstrekkeliget i større grad enn minimalitet.

[43] Se Bygrave, *Data protection law: approaching its rationale, logic and limits*, Dortrecht 2002, s 343-344.

fra deler av loven for personopplysninger som er «strengt pseudonymisert».[44] Forslaget er interessant i forhold til at det legges incentiver for utvikling og anvendelse av personvernøkende teknologi for å ivareta personvernet. Imidlertid er det uklart om man her tar sikte på bruk av pseudonymer i forbindelse med *transaksjoner*, eller om det er snakk om pseudonymisering av i utgangspunktet identifiserbare opplysninger (fasen «videre behandling» i figur 4.5). Etter min mening er begge tilnærminger viktige, men den første varianten vil, som vi har sett, være klart mer personvernøkende fordi den hindrer at det samles inn direkte identifiserbare opplysninger.

Mens minimalitetsprinsippet i liten grad er synliggjort i personopplysningsloven, er derimot prinsippet om datakvalitet gitt stor plass og tyngde. Prinsippet om datakvalitet fremgår av personopplysningsloven § 11, samt lovens formålsbestemmelse som uttrykker at loven skal bidra til at personopplysninger blir behandlet i samsvar med «grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og *tilstrekkelig kvalitet* på personopplysninger» (min kursivering). Når § 11 stiller krav til at opplysninger skal være «tilstrekkelige og relevante» og «korrekte og oppdaterte», må dette nødvendigvis også omfatte det forhold at opplysningene som er lagret gjelder rett person. Dette forutsetter imidlertid at den behandlingsansvarlige har tilstrekkelig gode rutiner for identifisering og autentisering. Etter som stadig mer samhandling skjer elektronisk er det grunn til å spørre om ikke lovgivningen burde være tydeligere på forskjellen mellom identifisering og autentisering, jf. kapittel 3.4 og 3.5. Lovens § 12 som regulerer bruk av fødselsnummer og andre entydige identifikasjonsmidler gir ikke klarhet i denne distinksjonen. Det er uklart om «entydige identifikasjonsmidler» her refererer til bruk av entydige identifikatorer og/eller bruk av autentiseringsmekanismer. En annen mulig tilnærming er å anse krav til identifisering og autentisering som et spørsmål om informasjonssikkerhet under betraktningen om at f.eks. utlevering av opplysninger vil være i strid med konfidensialitet eller tilgjengelighet. Dette blir imidlertid en for snever tilnærming siden spørsmålet om autentisering da først og fremst kommer på spissen i forhold til utlevering av opplysninger. Gode grunner taler derfor etter min mening for at distinksjonen klargjøres i § 11 eller i en ny revidert bestemmelse som skiller mellom adgangen til å benytte identifikatorer (f.eks. fødselsnummer) og hvilke krav som ellers stilles til autentisering.

5 Samlende synspunkter – veien videre

Den tradisjonelle tilnærmingen til PETs har vært minimalitet, det vil si tekniske og organisatoriske tiltak som tar sikte på å begrense adgangen til å identifisere den opplysningene gjelder. Forskningen og utviklingen innen personvernøkende identitetsforvaltning bryter ikke med PETs-tankegangen, men plasserer tradisjonelle PETs i et videre perspektiv som også omhandler sikker identifisering og autentisering.

Det er etter min mening viktig å opprettholde et skille mellom PETs og identitetsforvaltning på den ene siden og informasjonssikkerhetstiltak på den annen side. PETs og identitetsforvaltning retter fokuset på identitet og identifiserbarhet. Spørsmålet her er om det er nødvendig å samle inn identifiserende opplysninger i den enkelte transaksjon, eventuelt hvilken rolle eller identitet det er behov for å autentisere. Informasjonssikkerhetstiltak derimot tvinger oss ikke til å stille spørsmål *om* og med *hvilken identifiserbarhet* opplysninger skal innhentes og lagres. Her er fokuset kun på å sikre de opplysninger som er blitt lagret. Begge tilnærminger er selvsagt viktige. Faren ved kun å holde fast ved informasjonssikkerhetstilnærmingen er at man ikke legger noen begrensninger på hvilken informasjon som samles inn under dekke av at informasjonssikkerheten er tilstrekkelig. Den første tilnærmingen derimot, er personvernøkende i den forstand at den gir den enkelte bedre kontroll over egne opplysninger ved at mengden elektroniske spor og lagrede identifiserbare opplysninger holdes på et minimum. Ved vurdering av hvordan tekniske og organisatoriske tiltak kan støtte opp under personvernet, bør man derfor alltid starte med å vurdere spørsmål knyttet til identitet og identifiserbarhet (PETs/identitetsforvaltning), for deretter å vurdere relevante informasjonssikkerhetstiltak (f.eks. kryptering, tilgangskontroll etc).[45]

I fremstillingen av elektronisk kommunikasjon har siktemålet vært å synliggjøre hvordan personvernspørsmål knyttet elektroniske spor og

[44] Schartum og Bygrave, *Utredning av behov for endringer i personopplysningsloven*, 2006, radikalt forslag til ny § 3d.

[45] Det må antas at PETs vil kunne ha konsekvenser for informasjonssikkerhetsarbeidet ved at lagring av færre identifiserbare opplysninger medfører lavere sannsynlighet for og mindre konsekvenser av brudd på informasjonssikkerheten.

krav til identifisering kan håndteres under synsvinkelen identitetsforvaltning. Etter min mening er det her klargjørende å skille mellom de spørsmål om identitet og identifiserbarhet som kan relateres til den grunnleggende infrastrukturen for Internett (*kommunikasjonslaget*), og de spørsmål som må finne sin løsning i form av identitetsforvaltning i *tjenestelaget*. Det siste tiåret har vi vært vitne til en voldsom aktivitet, internasjonalt og nasjonalt, knyttet til utvikling av nye standarder og systemer for identitetsforvaltning. Disse løsningene og måten de implementeres på vil utvilsomt ha betydning for personvernet ettersom Internett blir en stadig viktigere kontaktflate mot omverdenen. I den forbindelse er det relevant å se hen til den satsningen som gjøres fra norske myndigheter med å legge til rette for nasjonalt ID-kort med eID.[46] Muligheten for sikker identifisering åpner for nye e-handel- og e-forvaltningstjenester. Imidlertid er det viktig å være bevisst på i hvilke tilfeller det vil være passende å stille krav til slik identifisering. Det faktum at man har eID som sikrer sterk autentisering av identitet betyr ikke at det bør benyttes i alle tilfeller. Fra et personvernsynspunkt er det dessuten betenkelig å legge opp til en sårbar infrastruktur med kun én eID-løsning. Det bør heller legges til rette for virksom konkurranse som gir valgfrihet mellom alternative identitetstilbydere.[47] Jeg vil holde fast ved det prinsipielle som ligger i at man i alle tilfeller starter med å stille spørsmål med hvilken påstand som skal autentiseres. Er identitet overhodet relevant? Eller holder det å få etablert tilstrekkelig sikkerhet for f.eks. en rolle eller en egenskap? Et eksempel på denne tilnærmingen finner man f.eks. hos Australske myndigheter som har utarbeidet et omfattende rammeverk som skal hjelpe forvaltningen med å finne frem til *hva* som skal autentiseres, samt til *hvordan* dette kan gjøres på en forholdsmessig og sikker måte.[48]

Det er gledelig å se at både EU og norske myndigheter uttrykker ønske om å støtte opp under personvernøkende teknologi, og ser dette som en viktig strategi for å kunne ivareta personvernet (jf. kapittel 1.3). Jeg mener det er all grunn til å legge videre trykk på de tiltakene som allerede er identifisert. EU kommisjonens strategi er, som nevnt, for det første å fremme *utvikling* av PETs, legge incentiver for næringslivets og offentlige myndigheters *anvendelse,* samt å heve folk flest sin *bevissthet* om PETs og personvernsspørsmål. Det er også god grunn til å følge opp Regjeringens IKT-melding som synliggjør utfordringene på dette området og som foreslår konkrete tiltak.[49] Det er ikke anledning til å diskutere disse tiltakene i detalj her. Jeg vil derfor heller rette oppmerksomheten mot en av hovedutfordringene – nemlig at PETs i liten grad har blitt tatt i bruk. Foreløpig har det vært liten etterspørsel etter PETs og få virksomheter har klart å gjøre godt personvern til et konkurransefortrinn. Grunnene til dette kan være mange, blant annet har det vært liten bevissthet blant virksomheter og forbrukere om hva som er personvernøkende og hva som ikke er det, og dermed har etterspørselen uteblitt. Den aktøren som synes best stilt til å endre denne situasjonen er det offentlige, som bør ha en klar ambisjon om å legge til rette for personvernøkende løsninger. Myndighetene har f.eks. anledning til å stille krav til at personvernhensyn blir et førende hensyn i utviklingsprosjekter og at dokumentering av personvernøkende design (ikke bare informasjonssikkerhet) løftes frem som et kriterium i anbudskonkurranser om levering av nye løsninger. Slike krav vil gi markedsaktørene incentiver til å satse på personvernøkende teknologi, noe som vil kunne føre til økt tilgjengelighet også i privat sektor. Viktigheten av det offentliges innsats og prioriteringer på dette området kan ikke understrekes sterkt nok. Det er etter min mening naivt å tro at markedsaktørene vil satse på PETs hvis ikke det offentlige går foran som et godt eksempel.

I IKT-meldingen er regelverksendring som gir mer direkte støtte til bruk av personvernøkende teknologi et av de foreslåtte tiltakene. Jeg mener det er grunn til å holde fast ved prinsippet om teknologinøytral lovgivning. Mer detaljerte krav eller anbefalinger til konkrete tekniske løsninger kan med fordel utarbeides innenfor konkrete sektorer, f.eks. som bransjevise normer, men hører nok ikke hjemme i den sentrale lovgivningen. Et aspekt som lovgiver med fordel bør vurdere å få tydeligere frem i lovgivningen er minimalitetsprinsippet. Som nevnt i kapittel 4.2.2 stiller personopplysningsloven ikke tydelige krav til eller føringer for minimalitet (anonymitet/pseudonymitet) i

[46] Justis- og politidepartementet, *Nasjonalt ID-kort*, Oslo, 2007.

[47] Dette synes å være gjengs oppfatning i identitetsforvaltningsmarkedet, se f.eks. Cameron, *Laws of Identity*, 2007, som fremhever "Pluralism of operators and technologies" som et av syv grunnprinsipper for identitetsforvaltning.

[48] Se Australian Government, *Australian Government e-Authentication Framework*, 2005.

[49] Se særlig kap 8.3.3 *Retten til å vere anonym*, 8.3.4 *eID og valfridom* og 8.3.5 *Utnytting av teknologien for å styrkje personvernet*.

transaksjoner. Ved tydeligere krav til minimalitet vil det f.eks. måtte dokumenteres hvorfor man har behov for å samle inn identifiserende opplysninger. Dette vil være å snu dagens situasjon på hodet hvor det selvsagte er at man behandler identifiserbare opplysninger. Et eksempel på en slik bestemmelse er å finne i Tysklands føderale personopplysningslov § 3a:

> «*§ 3 Data reduction and data economy*
> Data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data or as little personal data as possible. In particular, use is to be made of the possibilities for aliasing and rendering persons anonymous, in so far as this is possible and the effort involved is reasonable in relation to the desired level of protection.»

Som nevnt i kapittel 4.2.2 er det videre grunn til å se nærmere på om ikke personopplysningsloven bør innføre et tydelig skille mellom adgangen til å benytte bestemte identifikatorer (f.eks. fødselsnummer), og krav til autentisering og bruk av bestemte typer autentiseringsmekanismer (f.eks. biometri).

Avslutningsvis, etter å ha pekt på tiltak som krever en betydelig innsats og oppfølgning, kan det synes som vi har en lang vei å gå i forhold til å la personvernhensyn være med på å styre teknologiutvikling og -anvendelse. Det er nok dessverre også tilfellet. Samtidig er det mange og enkle tiltak som det er anledning til å gripe fatt i. Eksempelvis å følge lovens krav om å gi god informasjon om behandlingen av personopplysninger, samt å gjøre den enkelte kjent med sine rettigheter. Til syvende og sist handler dette om å heve bevisstheten om personvernspørsmål og PETs i alle ledd i næringskjeden – fra utviklere, til databehandlere og behandlingsansvarlige. Særlig trenger vi opplyste forbrukere og borgere som stiller krav og forventninger til virksomheters innsats på personvernområdet.

Bibliografi

Lovgivning, forarbeider mv

Personverndirektivet, 95/46/EF av 24. oktober 1995

Direktivet om personvern og elektronisk kommunikasjon, 2002/58/EF av 12. juli 2002

Datalagringsdirektivet, 2006/24/EF, av 15. mars 2006

Lov om behandling av personopplysninger (personopplysningsloven), lov 14. april 2000 nr 31

Lov om helseregistre og behandling av helseopplysninger (helseregisterloven), lov 18. mai 2001 nr 24

Lov om elektronisk kommunikasjon (ekomloven), lov 4. juli 2003 nr 83

Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften), forskrift 16. februar 2004

Forskrift om innsamling og behandling av helseopplysninger i Reseptbasert legemiddelregister (Reseptregisteret), forskrift 17. oktober 2003 nr 1246

Ot.prp. nr 49 (2005-2006) Om lov om endringer i helseregisterloven (Norsk pasientregister)

Artikkel 29-gruppen (WP 6/1997) anonymitet på Internett

Artikkel 29-gruppen (WP 68/2001) om autentiseringstjenester

St.meld. nr 17 (2006-2007) Eit informasjonssamfunn for alle

Tysklands føderale personopplysningslov, (Bundesdatenschutzgesetz), 15. november 2006

Bøker, artikler mv

Andresen, Herbjørn, «On Pseudonymous Health Registers: While they Work as Intended, they are Still Controversial in Norway», *Proceedings of the First International Conference on Health Informatics, Funchal, Madeira – Portugal*, Vol 1 (2008) 59-66

Australian Government, *Australian Government e-Authentication Framework*, (2005)

Boe, Erik, «Nye helseregistre inn bakveien?» *Kritisk juss*, Årg. 27, nr 1/2 (2000) 63-77

Brands, Stefan A., *Rethinking public key infrastructures and digital certificates: building in privacy*, (Cambridge, Mass. 2000)

Burkert, Herbert, «Privacy-enhancing technologies: typology, critique, vision», I: *Technology and privacy: the new landscape,* Agre, Philip og Rotenberg, Marc (red), (Cambridge, Mass. 1997)

Bygrave, Lee A., *Data protection law: approaching its rationale, logic and limits*, (Dortrecht 2002)

Bygrave, Lee A., «Privacy-Enhancing Technologies – Caught between a Rock and a Hard Place», *Privacy Law & Policy Reporter*, (2002) 135-137

Cameron, Kim, *Laws of Identity*, (2007)

Chaum, David, «Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms», *Communications of the ACM*, vol. 24 no. 2 (1981)

Clarke, Roger, *Identity Management* (Canberra 2004)

Datatilsynet, *E-forvaltning – Datatilsynets tilrådning til regjeringen*, Datatilsynets nettsted, (2007)

EU Commission, *First report on the implementation of the Data Protection Directive (95/46/EC)* (Brussel 2003)

European Commission, *Communication on Promoting Data Protection by Privacy Enhancing Technologies (PETs)* (Brussels 2007)

Hannemyr, Gisle, «Feil nummerbruk», *Lov&Data*, 92 (2007) 29-30

Hannemyr, Gisle, *Hva er internett*, (Oslo 2005)

Hansen, Marit et al., «Privacy-enhancing identity management», *Information Security Technical Report*, 1 (2004) 35-44

Justis- og politidepartementet, *Nasjonalt ID-kort*, Oslo, (2007)

Kent, Stephen T. og Millett, Lynette I., *Who goes there?: authentication through the lens of privacy*, (Washington, DC 2003)

L'Abée-Lund, Åsa, *Pseudonymisering av personopplysninger i sentrale helseregistre*, Oslo, (2006)

Lessig, Lawrence, *Code: version 2.0*, (New York 2006)

Mahler, Tobias og Olsen, Thomas, «Reputation Systems and Data Protection Law», I: *eAdoption and the Knowledge Economy: Issues, Applications, Case Studies,* Cunningham, Paul og Cunningham, Miriam (red), (Amsterdam 2004)

Norsk Regnesentral, *Elektroniske spor*, (Oslo 2005)

Olsen, Thomas og Mahler, Tobias, «Identity management and data protection law: Risk, responsibility and compliance in `Circles of Trust'», *Computer Law & Security Report*, 4 & 5 (2007) 342-351 & 415-426

Olsen, Thomas og Mahler, Tobias et al, *Identity management & Privacy*, Complex, (2007)

Olsen, Thomas, «Lovgivningsprosessen bak registreringsplikt for kontantkort til mobiltelefon», *Lov & Data*, 85 (2006) 1-6

Registratiekamer, IPC og TNO-FEL, *Privacy-enhancing technologies: the path to anonymity (Vols I & II)*, (1995)

Riisnæs, Rolf, *Digitale sertifikater og sertifikattjenester – roller, oppgaver og ansvar*, (Bergen 2007)

Schartum, Dag Wiese og Bygrave, Lee A., *Utredning av behov for endringer i personopplysningsloven* (Oslo 2006)

Schartum, Dag Wiese og Bygrave, Lee A., *Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger*, (Bergen 2004)

Søiland, Arne, «Sikrere mot id-tyveri», *Computer World*, 15.01.2007, sist nedlastet 02.06.2008

Tanenbaum, Andrew S., *Computer networks*, 4th (Upper Saddle River, N.J. 2003)

Teknologirådet, *Elektroniske spor og personvern* (Oslo 2005)

Øverlier, Lasse, *Anonymity, privacy and hidden services*, (Oslo 2007)

Nettsider

Australian Government e-Authentication Framework: http://www.agimo.gov.au/infrastructure/authentication/agaf_b/overview
Credentica: http://www.credentica.com
EPAL: http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/
EPIC, Privacy Tools: http://epic.org/privacy/tools.html
FIDIS: http://www.fidis.net/
GUIDE: http://istrg.som.surrey.ac.uk/projects/guide/
Jan Camenisch, IBM Zürich: http://www.zurich.ibm.com/%7Ejca/publications.html
P3P: http://www.w3.org/P3P/
Personvern på nettet, 6. november 2006, «Åpen høring om Norsk pasientregister»: http://www.personvern.uio.no/pvpn/nyheter.html
PET Workshop: http://petworkshop.org/
PICOS: http://www.picos-project.eu/
PRIME: https://www.prime-project.eu/
PRIMELIFE: http://www.primelife.eu/
TOR: http://www.torproject.org/

Norges offentlige utredninger 2008 og 2009

Statsministeren:

Arbeids- og inkluderingsdepartementet:
Om grunnlaget for inntektsoppgjørene 2008. NOU 2008: 10.
Yrkessykdommer. NOU 2008: 11.
Skift og turnus – gradvis kompensasjon for ubekvem arbeidstid. NOU 2008: 17.

Barne- og likestillingsdepartementet:
Kvinner og homofile i trossamfunn. NOU 2008: 1.
Kjønn og lønn. NOU 2008: 6.
Med barnet i fokus. NOU 2008: 9.

Finansdepartementet:
Kulturmomsutvalget. NOU 2008: 7.
Revisjonsplikten for små foretak. NOU 2008: 12.
Eierkontroll i finansinstitusjoner. NOU 2008: 13.
Om foretaksstyring og tiltak mot manipulering av finansiell informasjon. NOU 2008: 16.
Skadeforsikringsselskapenes virksomhet. NOU 2008: 20.

Fiskeri- og kystdepartementet:
Retten til fiske i havet utenfor Finnmark. NOU 2008: 5.

Fornyings- og administrasjonsdepartementet:
Individ og integritet. NOU 2009: 1.

Forsvarsdepartementet:

Helse- og omsorgsdepartementet:
Fordeling av inntekter mellom regionale helseforetak. NOU 2008: 2.

Justis- og politidepartementet:
Fra ord til handling. NOU 2008: 4.
Bourbon Dolphins forlis den 12. april 2007. NOU 2008: 8.
Barn og straff. NOU 2008: 15.
Fiskefartøyet "Western"s forlis 6. februar 1981. NOU 2008: 19.
Nettbankbasert betalingsoverføring. NOU 2008: 21.

Kommunal- og regionaldepartementet:

Kultur- og kirkedepartementet:

Kunnskapsdepartementet:
Sett under ett. NOU 2008: 3.
Fagopplæring for framtida. NOU 2008: 18.

Landbruks- og matdepartementet:

Miljøverndepartementet:

Nærings- og handelsdepartementet:

Olje- og energidepartementet:

Samferdselsdepartementet:

Utenriksdepartementet:
Samstemt for utvikling? NOU 2008: 14.

Offentlige publikasjoner

Opplysninger om abonnement, løssalg og pris får man hos:
Akademika AS
Avdeling for offentlige publikasjoner
Postboks 84 Blindern, 0314 OSLO
E-post: offpubl@akademika.no
Telefon: 22 18 81 00
Faks: 22 18 81 01
Grønt nummer: 800 80 960

Publikasjonen er også tilgjengelig på
www.regjeringen.no

MILJØMERKET
TRYKKSAK FRA 07 OSLO 241 344