NOU Norges offentlige utredninger 2022: 11

Ditt personvern – vårt felles ansvar

Tid for en personvernpolitikk

Norges offentlige utredninger 2022

Seriens redaksjon:
Departementenes sikkerhets- og serviceorganisasjon
Teknisk redaksjon

---

1. Cruisetrafikk i norske farvann og tilgrensende havområder
   Justis- og beredskapsdepartementet
2. Akademisk ytringsfrihet
   Kunnskapsdepartementet
3. På trygg grunn
   Olje- og energidepartementet
4. Grunnlaget for inntektsoppgjørene 2022
   Arbeids- og inkluderingsdepartementet
5. Myndighetenes håndtering av koronapandemien – del 2
   Statsministerens kontor
6. Nett i tide
   Olje- og energidepartementet
7. Et forbedret pensjonssystem
   Arbeids- og inkluderingsdepartementet
8. Ny minerallov
   Nærings- og fiskeridepartementet
9. En åpen og opplyst offentlig samtale
   Kultur- og likestillingsdepartementet
10. Inntektssystemet for kommunene
    Kommunal- og distriktsdepartementet
11. Ditt personvern – vårt felles ansvar
    Kommunal- og distriktsdepartementet

NOU Norges offentlige utredninger **2022: 11**

Ditt personvern – vårt felles ansvar

Tid for en personvernpolitikk

Utredning fra en kommisjon oppnevnt ved kongelig resolusjon 23. juni 2020.
Avgitt til Kommunal- og distriktsdepartementet 26. september 2022.

Departementenes sikkerhets- og serviceorganisasjon
Teknisk redaksjon

Oslo 2022

ISSN 0333-2306
ISBN 978-82-583-1511-4

07 Media AS

Til Kommunal- og distriktsdepartementet

Personvernkommisjonen ble oppnevnt ved kongelig resolusjon 23. juni 2020 for å vurdere personvernets stilling i Norge. Kommisjonen gir med dette sin utredning.

Oslo 26. september 2022

John Arne Moen
Leder

Ingvild Næss Nestleder	Haakon Hertzberg	Jill Walker Rettberg (frem til mars 2021)
Tor-Aksel Busch	Marianne Høyer	Dag Wiese Schartum
Trine Skei Grande	Finn Lützow-Holm Myrstad	Helge Veum
Trude Margrethe Haugli	Toril Nag	Brita Ytre-Arne (fra juni 2021)
	Oddhild Aasberg	

Catharina Nes
Sekretariatsleder

Janne Loen Kummeneje

Ailo Krogh Ravna

Innhold

1 Innledning og sammendrag 9
1.1 Personvern i nytt lys 9
1.1.1 Personvern på dagsorden 9
1.1.2 Personvern som samfunnsverdi ... 9
1.1.3 Teknologi og personvern er politikk 10
1.1.4 Teknologiutvikling på samfunnets premisser 10
1.2 En nasjonal personvernpolitikk 11
1.3 Sammendrag 12
1.3.1 Del I – Hva er personvern, rettslig rammeverk og teknologiske drivkrefter 12
1.3.2 Del II – Personvernets stilling og utfordringer innen utvalgte sektorer 13
1.3.3 Del III – Andre områder kommisjonen har arbeidet med 16

2 Kommisjonens mandat, sammensetning og arbeid 18
2.1 Personvernkommisjonens mandat 18
2.2 Personvernkommisjonens tolking og avgrensninger av mandatet 21
2.3 Kommisjonens sammensetning ... 22
2.4 Kommisjonens arbeid 23

Del I Hva er personvern, rettslig rammeverk og teknologiske drivkrefter 27

3 Hva er personvern og hvorfor er det viktig? 29
3.1 Hva er personvern 29
3.1.1 Personvern og personopplysningsvern 30
3.2 Ulike elementer i personvernet 30
3.3 Hvorfor er personvern viktig? 31
3.3.1 Hvorfor er personvern viktig for individet? 31
3.3.2 Hvorfor er personvern viktig for samfunnet? 31
3.3.3 Personvern på tvers av samfunnet 33

4 Rettslig regulering av personvern 34
4.1 Personvern som menneskerettighet 34
4.1.1 Grunnloven 35
4.1.2 Den europeiske menneskerettskonvensjonen artikkel 8 36
4.1.3 Barnekonvensjonen og barnets beste 36
4.2 Personopplysningsloven og personvernforordningen (GDPR) 37
4.2.1 Personvernforordningen 37
4.2.2 Hva gjelder personvernforordningen for? 38
4.2.3 Hvem gjelder personvernforordningen for? 38
4.2.4 Hvor gjelder personvernforordningen? 39
4.2.5 Personvernprinsippene 40
4.2.6 Behandlingsformål og behandlingsgrunnlag 40
4.2.7 Betydningen av risikovurderinger 41
4.2.8 Dokumentasjonsplikter 42
4.2.9 Virkemidler for å ivareta personvernet 42
4.3 Relevante kommende regelverk .. 43

5 Det teknologiske landskapet som påvirker personvernet 45
5.1 Teknologiske utviklingstrekk med betydning for personvernet .. 45
5.1.1 En digital hverdag 45
5.1.2 Teknologiske fundamenter for det digitale samfunnet 46
5.1.3 Samfunnssikkerhet i et digitalt samfunn 47
5.1.4 Personvernfremmende teknologi 49
5.2 Særskilt utfordrende eksempler på teknologianvendelser med implikasjoner for personvernet 50
5.2.1 Sporing og sammenstilling på tvers av plattformer og tjenester .. 50
5.2.2 Profilering og automatisert beslutningstaking 50
5.2.3 Biometrisk analyse og fjernidentifikasjon 52
5.2.4 Nevro- og bioteknologi 53
5.3 Personvernkommisjonens syn på forholdet mellom teknologisk og samfunnsmessig utvikling 54
5.3.1 Føre-var-prinsippet 55
5.4 Personvernkommisjonens anbefalinger oppsummert 55

Del II **Personvernets situasjon og utfordringer innen utvalgte sektorer** 57

6 **Personvern i den digitale forvaltningen** 59
6.1 Innledning 59
6.1.1 Hovedtrekk i digitaliserings-politikken 59
6.1.2 Viktigheten av tillit til offentlig forvaltning 61
6.2 Hvordan bruker offentlig forvaltning personopplysninger i en digital hverdag? 62
6.2.1 Hvordan digitaliseres den offentlige forvaltningen? 62
6.2.2 Automatisert rettsanvendelse 63
6.2.3 Maskinlæring 64
6.2.4 Forholdet mellom maskinlæring og profilering 65
6.2.5 Eksempler på bruk av maskin-læring i norsk og utenlandsk offentlig forvaltning 66
6.3 Rettslige rammer for behandling av personopplysninger i offentlig forvaltning 68
6.3.1 Legalitetsprinsippet og krav om rettsgrunnlag etter Grunnloven og EMK 68
6.3.2 Krav til behandlingsgrunnlag etter personopplysningsloven 69
6.3.3 Samlet om krav til lovregulering av behandlingsformål 70
6.3.4 Rettslige rammer for videre-behandling av personopplysninger i offentlig forvaltning 70
6.3.5 Vurdering av forenlighet 70
6.3.6 Andre rettslige skranker for bruk av opplysninger i offentlig forvaltning 71
6.4 Personvernutfordringer knyttet til deling og viderebehandling av personopplysninger i offentlig forvaltning 71
6.4.1 Fragmentert tilnærming til person-vern i offentlig forvaltning 71
6.4.2 Utforming av lovhjemler 73
6.4.3 Deling av personopplysninger mellom forvaltningsorganer 77
6.4.4 Bruk av kunstig intelligens 80
6.4.5 Profilering til kontrollformål 80
6.4.6 Offentlige aktører og store teknologiselskaper 81
6.4.7 Informasjonssikkerhet 83
6.5 Personvernkommisjonens anbefalinger oppsummert 84

7 **Personvern i justissektoren** 86
7.1 Innledning 86
7.1.1 Definisjoner, avgrensninger og metodologiske utfordringer 86
7.1.2 Personvern i justissektoren – en rettssikkerhetsgaranti 87
7.1.3 Viktigheten av tillit til justis-sektoren 88
7.2 Rettslig regulering av personvern i justissektoren 89
7.2.1 Kort om artikkel 8 i EMK og adgangen til å gjøre inngrep 89
7.2.2 Politiregisterloven 90
7.2.3 Domstolskontroll 92
7.2.4 Behandling av person-opplysninger i domstolene og kriminalomsorgen 92
7.3 Utviklingstrekk som påvirker personvernet 93
7.3.1 Endringer i kriminalitetsbildet 94
7.3.2 Økt internasjonalt samarbeid 94
7.3.3 Nye verktøy og metoder 95
7.3.4 Politiske føringer – utvidelser av politimyndighetenes inngreps-muligheter 95
7.4 Personvernutfordringer i justissektoren 96
7.4.1 Personvern i lovarbeid 97
7.4.2 Vurdering av personvern i myndighetsutøvelse 100
7.4.3 Åpenhet om politiets metodebruk 104
7.4.4 Effektiv domstolskontroll 105
7.4.5 Bruk av ny teknologi i justis-sektoren 105
7.4.6 Personvernkompetanse 110
7.4.7 Systemer og verktøy for å ivareta personvernet 112
7.4.8 Tilsyn og kontroll med behandlingen av person-opplysninger 114
7.5 Personvernkommisjonens anbefalinger oppsummert 115

8 **Personvern i skolen og barne-hagen** 118
8.1 Innledning 118
8.1.1 Avgrensninger, begreper og definisjoner 119
8.1.2 Politiske føringer for personvern i skolen og barnehagen 119
8.1.3 Tillit til skolens behandling av personopplysninger 121

8.2 Digitale løsninger i skolen 122
8.2.1 Hvilke applikasjoner blir elevene registrert i? 122
8.2.2 Prosess for anskaffelse av digitale løsninger i skolen 125
8.3 Rettslige rammer for behandling av opplysninger i skole og barnehage 125
8.3.1 Ansvarsplassering 126
8.3.2 Barnehageloven og opplæringslova 127
8.3.3 Bruk av samtykke 128
8.4 Personvernutfordringer i skole og barnehage i dag 128
8.4.1 Nasjonale føringer 129
8.4.2 Kompetanse og ressurser 131
8.4.3 Ansvar og rutiner 132
8.4.4 Bruk av elevers personopplysninger til kommersielle formål 134
8.4.5 Innkjøp og forhandlinger 137
8.4.6 Utvikling av digitale læringsverktøy 138
8.4.7 Undervisning i personvern 139
8.4.8 Barn og foresattes rettigheter 141
8.5 Personvernkommisjonens anbefalinger oppsummert 144

9 Forbrukernes personvern 147
9.1 Innledning 147
9.1.1 Begreper og definisjoner 147
9.1.2 Politiske føringer for ivaretagelse av forbrukernes personvern 148
9.2 Utviklingstrekk som påvirker forbrukernes personvern 149
9.2.1 Sosiale medier 150
9.2.2 Plattformøkonomien 150
9.2.3 Oppmerksomhetsøkonomien 151
9.2.4 Tingenes internett 151
9.2.5 Kunstig intelligens 151
9.2.6 Forbrukernes muligheter til å ivareta eget personvern 152
9.3 Rettslige rammer 154
9.3.1 Sektorlovgivning 154
9.3.2 Kommende europeisk regulering 155
9.4 Personvernutfordringer og konsekvenser 157
9.4.1 Tingenes internett muliggjør sporing overalt 158
9.4.2 Illegitim sporing og profilering 159
9.4.3 Manipulerende design 161
9.4.4 Informasjonsasymmetri 162
9.4.5 Diskriminering og manipulering .. 164
9.4.6 Svikt i markedet 166
9.5 Barn som forbrukere 171
9.5.1 Barns forbrukerhverdag 171
9.5.2 Barns rettigheter i digitale flater .. 171
9.5.3 Personvernutfordringer for barn som forbrukere 176
9.6 Personvernkommisjonens anbefalinger oppsummert 180

Del III Andre områder kommisjonen har arbeidet med 183

10 Regelkompleksitet og nasjonalt handlingsrom 185
10.1 Innledning 185
10.2 Et viktig, men vanskelig regelverk 185
10.3 Behov for å regulere personvern på nasjonalt nivå 187
10.3.1 Lovgivningspolitiske utgangspunkter 187
10.3.2 Klarere og mer utfyllende regulering av adgangen til å behandle personopplysninger ... 187
10.3.3 Klarere og mer utfyllende regulering av adgangen til å behandle særlige kategorier personopplysninger 188
10.3.4 Særlig om lovregulering av helt automatiserte, individuelle avgjørelser 189
10.3.5 Ideelle organisasjoners rett til å opptre på vegne av registrerte ... 190
10.3.6 Betydningen av tvil og fravær av regler i personvernforordningen ... 191
10.3.7 Tiltak for å forbedre lovtekster uten å gjøre innholdsmessige endringer 191
10.4 Personvernkommisjonens anbefalinger oppsummert 192

11 Teknologi i personvernets tjeneste 194
11.1 Teknologi som problem og løsning 194
11.2 Grunnleggende om personvernteknologi 194
11.3 Beskyttelse mot å bli registrert eller være registrert 196
11.4 Særskilt om innebygd personvern 197
11.4.1 Overordnet presentasjon 197
11.4.2 Rettslige krav til innebygd personvern 198
11.4.3 Eksempel på helhetlig innbygging av personvern 199

11.4.4 Personvernkommisjonens vurderinger av innebygd personvern 200
11.5 Personvernkommisjonens anbefalinger oppsummert 201

12 Åpenhet 202
12.1 Innledning 202
12.2 Forholdet til ytringsfriheten 203
12.3 Nedkjølende effekt av manglende åpenhet 203
12.4 Den menneskelige faktoren 203
12.5 Medvirkning 204
12.6 Åpenhet om håndheving av personvernregelverket 205
12.7 Hvordan kan åpenheten bli bedre? 205
12.8 Personvernkommisjonens anbefalinger oppsummert 208

13 Veiledning, tilsyn og klage 209
13.1 Bakgrunn og premisser 209
13.2 Datatilsynet – myndighet, oppgaver og organisering 210
13.2.1 Myndighet og oppgaver 210
13.2.2 Ledelse, budsjett og årsverk 211
13.2.3 Europeisk samarbeid i saksbehandlingen 212
13.2.4 Personvernnemnda 213
13.3 Innledende vurderinger av forutsetninger for god etterlevelse av personvernregelverket 213
13.3.1 Samarbeid mellom tilsyn 214
13.4 Spesielt om behov for veiledning ... 215
13.4.1 Datatilsynets veiledningsvirksomhet 215
13.4.2 Forhåndsdrøftelser 216
13.4.3 Om behovet for veiledning 216
13.4.4 Forholdet mellom Datatilsynets veiledning og tilsyns-/ kontrollvirksomhet 217
13.4.5 Regulatoriske sandkasser 218
13.4.6 Behov for veiledning fra andre myndigheter 219
13.4.7 Betydningen av forvaltningens alminnelige veiledningsplikt 220
13.4.8 Veiledning i regi av bransjeorganisasjoner, fellesfunksjoner innen offentlig forvaltning med flere 220
13.5 Behov for tilsyn fra andre tilsynsmyndigheter 221
13.6 Datatilsynets rolle ved utforming av lov og forskrifter 221
13.7 Spesielt om behandling av klager fra registrerte 222
13.7.1 Oversikt 222
13.7.2 Synligheten av registrertes rett til å klage til Datatilsynet 223
13.8 Personvernkommisjonens anbefalinger oppsummert 225

14 Økonomiske og administrative konsekvenser 227
14.1 Innledning 227
14.2 Den digitale forvaltningen 227
14.3 Justissektoren 228
14.4 Skole- og barnehagesektoren 228
14.5 Forbrukerområdet 229
14.6 Andre områder 229

Referanser og litteratur 231

Digitale vedlegg

Ericson, I. S. (2022). *Barns samtykkekompetanse på personvernfeltet.* Utredning for Personvernkommisjonen.

Lintvedt, M. N. (2022). *Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering.* Utredning for personvernkommisjonen.

Kapittel 1
Innledning og sammendrag

1.1 Personvern i nytt lys

I denne utredningen tegner *Personvernkommisjonen* et bilde av en digitaliseringsprosess som preger alle samfunnssektorer. Det er et tverrpolitisk mål å digitalisere, og dette arbeidet har skjedd og vil trolig fortsette å skje i høyt tempo. Siden den forrige *personvernkommisjonen* la fram sin utredning, har det vært gjennomført en rekke omfattende digitaliseringsprosesser i offentlig og privat sektor. Det har medført at stadig flere personopplysninger samles inn, brukes og viderebrukes. Samfunnsgevinstene av digitaliseringen er ofte store, og bruken av personopplysninger bidrar til både gode og effektive tjenester for innbyggerne. Samtidig ser *Personvernkommisjonen* en gjennomgående tendens til at digitaliseringen skjer på bekostning av personvernet. *Personvernkommisjonen* har gjennom arbeidet med utredningen etterstrebet å få et overblikk over denne utviklingen, og å peke på mulige veier fremover for å sikre og styrke personvernet i det digitale samfunnet.

1.1.1 Personvern på dagsorden

Personvern handler om hvilket samfunn vi ønsker å leve i, i dag og i dagene som kommer. På tross av dette, betraktes personvern i mange tilfeller som et ekspertfelt eller nisjeområde. Personvern diskuteres ofte i kontekst av paragrafer, lovfortolkning og etterlevelse. For profesjonelle aktører er personvern gjerne forbundet med formelle krav, mulige sanksjoner og vanskelige juridiske vurderinger som kommer i veien for utførelsen av daglige oppgaver. Folk flest forbinder kanskje personvern med irriterende samtykkeforespørsler som stadig må klikkes på, e-poster om oppdaterte personvernerklæringer som aldri leses, og lignende forstyrrelser som tar oppmerksomhet bort fra andre gjøremål.

I samtaler med elever i grunnskolen kom det frem at elevene er lei av å snakke om personvern som noe som handler om pekefingre og forbud.[1] Elevene ønsker en åpen og reflektert samtale om hvordan personopplysninger samles inn, hva de brukes til, hvordan slik innsamling påvirker oss og hvilke effekter det har på samfunnet. Slike samtaler forutsetter en bredere diskusjon om hva personvern betyr for samfunnet som helhet, og hva samfunnet risikerer å miste dersom personvernet ikke ivaretas.

Etter *Personvernkommisjonens* syn er det på høy tid at diskusjoner rundt personvern løftes ut fra ekspertsirklene og gjøres til et relevant og viktig spørsmål i samfunnsdebatten, i kommunestyrer og på Stortinget. For at dette skal kunne skje, må personvernet anerkjennes som et samfunnsgode som har en grunnleggende verdi. Personvernet må forstås og vurderes i positiv forstand, som en verdi som bidrar til å ivareta og bygge tillit i samfunnet, i stedet for en bremsekloss eller et nødvendig onde for å unngå sanksjoner.

1.1.2 Personvern som samfunnsverdi

Et godt personvern legger grunnlaget for ytringsfrihet, informasjonsfrihet og meningsdannelse. Personvern er med andre ord en forutsetning for et åpent samfunn og et velfungerende demokrati.

Personvern kan bidra til en bedre maktbalanse mellom individer, grupper, myndigheter og private aktører. Innsamling, sammenstilling og bruk av personopplysninger innebærer at enkelte aktører får stor innflytelse. Det ligger mye makt i å ha inngående kunnskap om, og potensielt kunne benytte opplysninger om, personers liv, tanker og hemmeligheter. Personopplysninger kan blant annet anvendes til å skreddersy budskap, treffe beslutninger basert på antagelser om individer og grupper, og til å utvikle nye tjenester. Kunnskap om og mulighet til å kontrollere hva andre vet om oss, og hvordan de kan bruke data om oss, er et viktig virkemiddel for å begrense denne makten.

Personvern handler ikke kun om individers rettigheter og valgmuligheter. Godt personvern hand-

[1] Falch, C. (2022). *Rapport til Personvernkommisjonen. Intervjuer med barn og unge om personvern.*

ler også om å verne andre, for eksempel ved å skjerme utsatte grupper for utilbørlige inngrep, eller ved å sikre at alle innbyggere har reelt vern uavhengig av kompetanse og ressurser. Dermed er personvern også en kollektiv og solidarisk verdi. For at personvern i praksis skal bli ivaretatt som en grunnleggende samfunnsverdi, må politikere og andre beslutningstakere se personvernet som en verdi det er ønskelig å ivareta. Det betyr at teknologioptimisme må ledsages – og av og til dempes – av kritiske refleksjoner rundt hva teknologiutvikling kan bety for samfunnet vårt. Det handler dessuten om å velge teknologiske løsninger som har bygget inn og gir mulighet for å ivareta personvernet. Kritiske refleksjoner forutsetter grunnleggende forståelse av både teknologien og de juridiske problemstillingene, men i bunn og grunn handler det om å forstå og vektlegge menneskerettigheter i møte med teknologi.

1.1.3 Teknologi og personvern er politikk

Teknologi kan i mange tilfeller ha endringskraft, med effekter på hvordan vi lever, hvordan vi oppfatter oss selv, og hvordan vi eksisterer i samspill med andre. Endringer som har utspring i teknologisk utvikling kan fremstå som revolusjonerende, på godt og vondt. Samtidig skjer disse endringene ofte gradvis, og eventuelle problemstillinger dukker i mange tilfeller ikke opp før i ettertid.

Personvernet er ofte usynlig, i den forstand at det ikke legges merke til før noe går galt, og til og med når krenkelser skjer, er de sjeldent ledsaget av fysisk merkbare konsekvenser. Det leder til at en utvikling som kan endre samfunnet på grunnleggende måter ofte gjennomføres uten at det reises kritiske spørsmål om hvorvidt utviklingen er ønsket, og uten at utviklingen er gjenstand for en åpen demokratisk debatt.

Det er ikke realistisk at det brede lag av befolkningen skal ha omfattende kunnskap om og kompetanse på de teknologiske og juridiske problemstillingene som er del av mange personverndiskusjoner. Arbeidet med å iverksette forebyggende tiltak og beskytte innbyggerne mot brudd på personvernet, må ledes av myndighetene. Likevel forutsetter endringskraften teknologi kan ha på samfunnet, at de fleste, som en del av å være en opplyst samfunnsdeltaker, bør ha en grunnleggende forståelse for hvilken rolle personvernet spiller i samfunnsutviklingen.

Utvikling og innføring av ny teknologi skjer i et hurtig tempo, og teknologi som fremstår som kontroversiell eller virkelighetsfjern i dag kan normaliseres og bli allment akseptert i fremtiden. Når dette skjer, kan det innebære en gradvis svekkelse av personvernet. Denne svekkelsen kan være vanskelig å få øye på før det er for sent å motvirke de negative effektene. Teknologiutviklingen og konsekvensene av den vil i mange tilfeller være uforutsigbare, og eventuelle skadevirkninger kan være vanskelige å motvirke dersom teknologien allerede er tatt i utstrakt bruk. For å motvirke en negativ utvikling er det derfor viktig med demokratiske diskusjoner om hvilke inngrep i folks rettigheter og friheter samfunnet skal akseptere.

1.1.4 Teknologiutvikling på samfunnets premisser

Å prioritere personvernet som en samfunnsverdi er ikke nødvendigvis enkelt eller friksjonsfritt. På kort sikt kan det innebære å stenge døren for enkelte teknologiske virkemidler som kan være både gode og nyttige. Samtidig kan nye dører for innovasjon og utvikling av alternativ teknologi tuftet på våre demokratiske verdier og prinsipper bli åpnet. Det vil ha en stor verdi for samfunnsutviklingen på sikt.

Personvernkommisjonen er også opptatt av at teknologi kan brukes bevisst for å oppnå et bedre personvern. Teknologiske hjelpemidler kan for eksempel hjelpe folk til både å forstå hvilke rettigheter de har, og hjelpe dem med å bruke dem. *Personvernkommisjonen* mener slike teknologiske muligheter hittil ikke er brukt i tilstrekkelig grad.

For å tilrettelegge for ansvarlig teknologiutvikling og innovasjon, må personvernet ivaretas gjennom konkrete handlinger hos myndigheter og virksomheter som behandler personopplysninger. I denne utredningen presenterer *Personvernkommisjonen* en rekke tiltak for å bidra til handling og forbedring. Noen av tiltakene kan gjennomføres ved politiske og forretningsmessige grep, mens andre krever kultur- og kompetansebygging over tid. Felles for tiltakene er at de vil bidra til å løfte bevisstheten om personvern.

Det er *Personvernkommisjonens* ønske og håp at utredningen vil stimulere til en bredere samfunnsdebatt om personvernet. Det innebærer både ovennevnte diskusjon om hvilke inngrep i personvernet samfunnet skal akseptere, men også at problemstillingene belyses fra et politisk perspektiv. Slik kan disse grunnleggende demokratiske spørsmålene løftes ut av rene juridiske eller teknologiske drøftelser, og ses i et bredt samfunnsmessig, politisk og menneskerettslig perspektiv.

1.2 En nasjonal personvernpolitikk

Personvernkommisjonen etterlyser en nasjonal personvernpolitikk som legger føringer for digitaliseringen av samfunnet i tillegg til hva som følger av lovgivningen. Politikken må omfatte både offentlig og privat sektors behandling av personopplysninger, og må sørge for at personvern ivaretas i utformingen av lovverk.

Regjeringen bør utforme en nasjonal personvernpolitikk som ser på personvernets status i Norge i dag og i tiden som kommer. Personvern er et felles ansvar. Derfor må personvernpolitikken bidra til å åpne opp en offentlig samtale om personvern, og gjøre den til en inkluderende og viktig debatt om grunnleggende verdier, samfunn og demokrati.

Nedenfor oppsummerer *Personvernkommisjonen* hvilke *overordnede hensyn* som må inngå i en nasjonal personvernpolitikk. Disse punktene suppleres med eksempler på konkrete anbefalinger fra *kommisjonen*, hentet fra de ulike delkapitlene i utredningen.

En nasjonal personvernpolitikk må ha som overordnet mål å sørge for reell ivaretakelse av personvernet. Politikken må gi føringer på tvers av sektorer, i den hensikt å ivareta innbyggernes personvern. Det krever formulering av overgripende prinsipper for hvordan samfunnet kan ivareta personvernet som en naturlig del av digitaliseringen. Utviklingen av politikken må skje i åpne samfunnsdebatter om prinsipielle spørsmål knyttet til hvor store inngrep i personvernet innbyggerne skal måtte tåle, for eksempel for å imøtekomme ønsket om effektiv forvaltning og kriminalitetsbekjempelse. *Personvernkommisjonen* anbefaler at *føre-var-prinsippet* anvendes i tilfeller hvor teknologianvendelse innebærer særlig høy risiko for personvernet.

En nasjonal personvernpolitikk må se personvernet i et helhetlig perspektiv. Det finnes i Norge i dag ingen offentlig virksomhet som har et overordnet ansvar for å vurdere den samlede bruken av personopplysninger i offentlig forvaltning, og betydningen denne har for personvernet. Vurderinger knyttet til bruk av personopplysninger foretas i stor grad sektorvis, ofte med liten grad av parlamentarisk kontroll og åpen debatt. Så lenge personvernvurderinger gjøres i siloer, eller stykkevis og delt, er det svært vanskelig å vurdere den samlede effekten av potensielt inngripende tjenester, tiltak eller lovendringer. Regjeringen bør ha særlig oppmerksomhet på personvernkonsekvensene av mer utstrakt deling og viderebehandling av personopplysninger, og hvordan dette skal vurderes opp mot andre viktige hensyn som effektivisering og rettssikkerhet. For å rette oppmerksomhet mot viktigheten av å ivareta personvernet i digitaliseringen av samfunnet, mener *Personvernkommisjonen* at regjeringen årlig bør legge frem en personvernpolitisk redegjørelse for Stortinget, forankret i gjeldende personvernpolitikk.

En nasjonal personvernpolitikk må innebære grundige risikovurderinger. Det er ikke nok å vurdere personvernkonsekvenser kun i forbindelse med den enkelte konkrete behandlingen av personopplysninger. Mulige personvernkonsekvenser må også utredes ved utforming av regelverk, ved utviklingen av tjenester og ved utarbeidelse av budsjetter, rutiner og organisatoriske tiltak. Personvernvennlige teknologiske og organisatoriske alternativer må alltid utredes før det forutsettes et motsetningsforhold mellom personvern på den ene side og for eksempel samfunnssikkerhet, kriminalitetsbekjempelse og effektivitet på den annen side.

En nasjonal personvernpolitikk må ha særlig oppmerksomhet på sårbare grupper, herunder barn og unge. Sårbare grupper kan ha dårligere forutsetninger for å ivareta eget personvern og å utøve sine rettigheter. Feil bruk av personopplysninger kan bidra til å skape eller forsterke urettmessige skjevheter som særlig rammer utsatte individer og grupper. Barn og unge er en særlig sårbar gruppe, fordi de i større grad enn voksne formes av sine omgivelser og utforsker sin identitet. Derfor er det viktig at ikke personopplysninger om dem anvendes til å sette dem i bås, eller brukes mot dem senere i livet. *Personvernkommisjonen* anbefaler derfor at regjeringen arbeider for et forbud mot atferdsbasert markedsføring rettet mot barn. Skole- og barnehagesektoren må gå foran for å etterstrebe at personvernet ivaretas. Det er uakseptabelt at barns personopplysninger blir gjenstand for kommersiell utnyttelse.

En nasjonal personvernpolitikk må inkludere en tydelig utenrikspolitisk rolle. Norge bør innta en aktiv rolle i utformingen av nye internasjonale regelverk, samt i utviklingen av internasjonale standarder og fellesløsninger som kan fremme personvernet. Det innebærer at representanter fra norske myndigheter arbeider aktivt og systematisk opp mot europeiske lovprosesser som vil ha konsekvenser for personvernet.

En nasjonal personvernpolitikk må utnytte det nasjonale handlingsrommet for regulering. I mange tilfeller er det begrensninger i Norges handlingsrom når det gjelder utforming av regler og prosedyrer som berører personvernet. Internasjonale myndigheter, med EU i sentrum, legger i stor

grad føringer for hva som er mulig å gjennomføre på nasjonalt nivå. Likevel er det relativt stort rom for nasjonalt tilpassede bestemmelser. Norske myndigheter må føre en aktiv nasjonal lovgivningspolitikk for å fremme personvern. Det bør alltid være en ambisjon å bruke det nasjonale handlingsrommet som EU-lovgivningen gir, både for å *supplere* de europeiske reglene, *støtte opp under* og for å *styrke* gjeldende EU-lovgivning som norske myndigheter ser som spesielt viktig. Eventuelt bør norske myndigheter vedta *avvikende norske regler* dersom det er adgang og tilstrekkelig grunn til det.

En nasjonal personvernpolitikk må fremme personvernvennlig innovasjon. Teknologiutvikling bør skje på en måte som ivaretar og fremmer personvernet. *Personvernkommisjonen* mener at det bør utvikles robuste standarder og normer for å tydeliggjøre hvordan innovasjon kan skje innenfor etiske og forsvarlige rammer. Den nasjonale personvernpolitikken bør også styrke forskning og utvikling på personvernfeltet, for å bidra til personvernvennlig innovasjon og digitalisering. Forskning på personvernfeltet vil kunne ha stor betydning for vår evne til å forstå de samlede konsekvensene av digitaliseringen for innbyggernes grunnleggende rettigheter og friheter.

En nasjonal personvernpolitikk må innebære at offentlig sektor går foran. Offentlige myndigheter har et ansvar for å holde en høy standard, også når det gjelder personvern. Det innebærer at offentlige myndigheter må gjøre grundige personvernvurderinger og ta i bruk verktøy som respekterer innbyggernes personvern. *Personvernkommisjonen* anbefaler at offentlig sektor bruker sin innkjøpsmakt for å stimulere til fremveksten av personvernvennlige produkter og tjenester. Det bør gis føringer om hvordan personvern bør vektes i anskaffelser.

En nasjonal personvernpolitikk forutsetter et solid kunnskaps- og kompetansegrunnlag. Beslutninger og vurderinger som påvirker personvernet må tuftes på juridisk, teknologisk og samfunnsvitenskapelig kompetanse. Derfor mener *Personvernkommisjonen* at offentlig sektor må prioritere å styrke personvernkompetansen blant sine ansatte. Personvernpolitikken må også inneholde tiltak som sørger for at innbyggerne får grunnleggende opplæring i personvern. *Personvernkommisjonen* anbefaler derfor at personvern blir en del av grunnskoleutdanningen, og at undervisning i personvern styrkes på alle nivå, inkludert høyere utdanning.

En nasjonal personvernpolitikk forutsetter åpenhet rundt behandling av personopplysninger. Åpenhet rundt bruk av personopplysninger er nødvendig for å ivareta og bygge opp innbyggernes tillit til myndighetene, og forbrukernes tillit til tjenesteleverandører. Dette innebærer åpenhet om hvilke personopplysninger som behandles og brukes om individer, men også åpenhet rundt hvordan personopplysninger aggregeres/sammenstilles og viderebrukes. Opplysningene bør i størst mulig grad være tilgjengelige for innbyggerne, uten at de aktivt må be om innsyn.

En nasjonal personvernpolitikk forutsetter effektiv håndheving. For å sikre at regelverk ment for å beskytte innbyggernes personvern etterleves, er det nødvendig at Datatilsynet har tilstrekkelige ressurser for å håndheve loven. I tillegg til effektive kontroller og sanksjoner, mener *Personvernkommisjonen* at Datatilsynet må ha ressurser til veiledning av aktører med behov for det. Siden personvern stadig omfatter flere og større områder, må tilsynet styrkes i tråd med disse faktiske behovene. *Kommisjonen* mener videre at også andre tilsynsmyndigheter enn Datatilsynet bør veilede om personvernspørsmål som direkte er knyttet til deres myndighetsområde

1.3 Sammendrag

De følgende avsnittene gir et sammendrag av hovedpunktene i hvert enkelt kapittel i utredningen. *Personvernkommisjonen* står samlet bak vurderingene og anbefalingene, med unntak av en anbefaling i kapittel 9 knyttet til å utrede et generelt forbud mot atferdsbasert reklame. Her har *kommisjonen* delt seg i et *flertall* som støtter anbefalingen og et *mindretall* som ikke støtter dette tiltaket.

1.3.1 Del I – Hva er personvern, rettslig rammeverk og teknologiske drivkrefter

I *kapittel 3* gjør *Personvernkommisjonen* rede for forskjellige oppfatninger av hva personvern betyr, og drøfter hvorfor personvern er viktig både for individet og for samfunnet.

Personvern er en grunnleggende rettighet for individet, og er blant annet et viktig premiss for ytringsfrihet. Samtidig har personvern et kollektivt aspekt. Dersom personvernet tilsidesettes, kan det ramme sårbare grupper eller samfunnet som helhet, for eksempel ved at grupper legger bånd på seg og demper sin aktive samfunnsdeltagelse. Derfor kan ikke ansvaret for personvern utelukkende overlates til individuelle valg og pre-

feranser. Denne diskusjonen danner bakteppet for resten av utredningen.

I *kapittel 4* gjennomgår *Personvernkommisjonen* den rettslige reguleringen av personvernet. Det gis en overordnet oversikt over de viktigste bestemmelsene i personvernforordningen, samt en gjennomgang av reguleringen av personvern som menneskerettighet og i Grunnloven. *Kommisjonen* gjør også kort rede for hvordan personvernet berøres og reguleres i ulike sektorregelverk. I tillegg går *Personvernkommisjonen* gjennom den særskilte reguleringen av barns personvern, herunder Grunnloven og barnekonvensjonen. Prinsippet om barnets beste presenteres kort. Avslutningsvis i kapitlet tar *kommisjonen* for seg gjeldende og kommende europeisk regelverk på personvernområdet. Omtale av andre regelverk og mer mer detaljert regelverksgjennomgang er plassert i de respektive kapitlene.

I *kapittel 5* presenterer *Personvernkommisjonen* en kortfattet oversikt over grunnleggende trekk ved teknologiutviklingen i samfunnet, og identifiserer noen nøkkelområder hvor teknologien kan skape særlige personvernutfordringer. Denne beskrivelsen legger grunnlaget for videre drøftelser i påfølgende kapitler.

Utviklingen av kraftig sporings- og sensorteknologi, infrastruktur for overføring av data, lagringsteknologi, samt økt prosessorkraft har gjort det mulig å samle inn, overføre, lagre og behandle data i stor skala. Det har ført til at stadig større mengder personopplysninger kan samles inn og analyseres, en utvikling som setter personvernet under press. Den hurtige og kompliserte teknologiutviklingen har ført til at beslutningstagere og lovgiver ofte kommer «bakpå». For å motvirke en uheldig utvikling, er det derfor viktig med en prinsipiell og kunnskapsbasert tilnærming til hvordan teknologien påvirker samfunnet, og hvordan samfunnet kan påvirke teknologiutviklingen. Diskusjonen rundt teknologiutvikling må også omfatte røde linjer – teknologi eller teknologianvendelse som er *uakseptabel* i et demokratisk samfunn.

Personvernkommisjonen tar til orde for at førevar-prinsippet må komme til anvendelse før innføringen av teknologi som kan ha alvorlige konsekvenser for individer og samfunnet. På bakgrunn av dette anbefaler *kommisjonen* et forbud mot bruk av biometrisk fjernidentifikasjon i det offentlige rom. Dette er teknologi for å identifisere individer i sanntid, og er etter *Personvernkommisjonens* syn så inngripende at teknologien ikke er forenlig med grunnleggende samfunnsverdier og menneskerettigheter.

1.3.2 Del II – Personvernets stilling og utfordringer innen utvalgte sektorer

Personvernkommisjonens mandat fremhever flere konkrete områder/sektorer hvor personvernutfordringene er mange og vanskelige. *Kommisjonen* er i mandatet bedt om å ha særskilt fokus på spørsmål som gjelder personvern i offentlig sektor, personvern i justissektoren, personvernet til forbrukere, samt barn og unges personvern. I utredningens del II presenteres *Personvernkommisjonens* vurderinger og forslag til tiltak innenfor de ovennevnte områdene.

Personvernkommisjonen anbefaler, som nevnt ovenfor, at regjeringen etablerer en personvernpolitikk som ses i sammenheng med digitaliseringspolitikken. I personvernpolitikken bør regjeringen ha særlig oppmerksomhet på personvernkonsekvensene av mer utstrakt deling og viderebehandling av personopplysninger, og hvordan slik deling og viderebehandling skal vurderes opp mot andre viktige hensyn som effektivisering og rettssikkerhet. Regjeringen bør årlig legge frem en personvernpolitisk redegjørelse for Stortinget, forankret i gjeldende personvernpolitikk.

I *kapittel 6* drøfter *Personvernkommisjonen* digitaliseringen av offentlig forvaltning, og vurderer personvernkonsekvenser ved utviklingen. Offentlig sektor har et særlig ansvar for å sørge for at innbyggernes personvern ivaretas, og må derfor tilrettelegge for både grundige konsekvensvurderinger og rettssikkerhetsgarantier. Dersom forvaltningen ikke evner å ivareta innbyggernes personvern på en tilstrekkelig måte, kan dette få alvorlige konsekvenser for den enkelte, og kan svekke tilliten til myndighetene.

Den digitale forvaltningen har som mål å kunne tilby effektive og brukervennlige tjenester. Som en del av denne målsetningen blir en rekke forvaltningsoppgaver helt eller delvis automatisert, blant annet ved at automatiserte systemer brukes i saksbehandlingen. Dette innebærer gjerne at systemet analyserer store mengder opplysninger om innbyggerne for å utlede anbefalinger om vedtak. Selv om bruken av slike systemer i forvaltningen medfører en rekke fordeler, kan det oppstå personvernutfordringer dersom systemene ikke legger til rette for en forståelig og gjennomsiktig saksbehandling. *Personvernkommisjonen* drøfter særlig utfordringer knyttet til bruk av automatiserte systemer til kontrollformål. Utstrakt eller uforholdsmessig bruk av profilering til kontrollformål kan ha alvorlige negative effekter på individer og samfunnet, for eksempel i form av ulovlig forskjellsbehandling eller nedkjølingsef-

fekter. *Personvernkommisjonen* anbefaler derfor at offentlig forvaltning bør anvende føre-var-prinsippet ved bruk av profilering til kontrollformål.

Det er også personvernutfordringer knyttet til utformingen av regelverk i offentlig sektor. Dersom personvernkonsekvenser ikke utredes i tilstrekkelig grad som en del av regelverksarbeid, risikerer man at det legges til rette for uforholdsmessig store inngrep i personvernet. *Personvernkommisjonen* anbefaler derfor at det iverksettes systematiske personvernvurderinger i lovarbeider.

I kapitlet gir *Personvernkommisjonen* også en oversikt over de rettslige rammene for behandling av personopplysninger i offentlig forvaltning. *Kommisjonen* presenterer deretter de ulike kravene til behandlingsgrunnlag. Det gis et overblikk over behandlingsgrunnlag, behandlingsformål og rettslige rammer for viderebehandling av personopplysninger. *Personvernkommisjonen* fremhever at det særlig er viktig å skape trygge og klare rettslige rammer for viderebehandling av personopplysninger. *Personvernkommisjonen* mener at konsekvensutredninger i lovarbeid bør inkludere vurderinger av om eksisterende regelverk er tilstrekkelig, og om det nasjonale handlingsrommet skal anvendes. Dersom det fastsettes nasjonale bestemmelser, kan dette bidra til klarere og mer utfyllende regelverk, og dermed gi større forutberegnelighet for innbyggerne. I tillegg gir det bedre grunnlag for å vurdere om en konkret behandling av personopplysninger er lovlig.

Personvernkommisjonen trekker frem flere utfordringer knyttet til deling og bruk av personopplysninger i offentlig forvaltning. Utforming av lovhjemler, bruk av kunstig intelligens og deling av personopplysninger mellom forvaltningsorganer er noen av utfordringene som gjennomgås. En utfordring ved deling av personopplysninger på tvers av organer, er at det oppstår usikkerhet rundt *ansvarsforholdene* mellom samarbeidende organer. *Personvernkommisjonen* anbefaler derfor at ansvarsfordelingen i større grad bør lov- eller forskriftsfestes der deling av personopplysninger inngår som en del av et større samarbeid mellom forvaltningsorganer og hvor uklarhet kan medføre alvorlige personvernkonsekvenser.

Personvernkommisjonen mener det er behov for et rådgivende organ som kan ha et helhetlig overblikk over bruk av personopplysninger i Norge. Et slikt organ kan bidra til at den til enhver tid gjeldende personvernpolitikken iverksettes og gjennomføres på en god måte og gi råd om hvordan hensynet til personvern skal vektes mot andre hensyn, samt hvilke etiske vurderinger som bør gjøres i forbindelse med bruk av personopplysninger.

I *kapittel 7* ser *Personvernkommisjonen* på personvernutfordringer i justissektoren, med særlig blikk på politiets behandling og bruk av personopplysninger. På justisområdet må retten til personvern i mange tilfeller veies opp mot hensynet til effektiv kriminalitetsbekjempelse, som betyr at personvernet settes under press. Personvernet utfordres både når nye metoder ønskes tatt i bruk, og når det iverksettes lovarbeider som skal tilrettelegge for kriminalitetsbekjempelse og forebygging.

Ved utforming av regelverk vurderes personvernkonsekvenser gjerne i begrenset grad, eller ikke i det hele tatt. Dette kan føre til at en rekke tilsynelatende mindre inngripende hjemler innføres, noe som samlet kan skape et overvåkningstrykk på befolkningen. Dersom det gjennomføres uforholdsmessig inngripende tiltak i kriminalitetsbekjempelsens navn, vil det både kunne svekke tilliten til sentrale samfunnsinstitusjoner og skape nedkjølingseffekter som kan utfordre grunnleggende demokratiske verdier.

Etter *Personvernkommisjonens* oppfatning er det derfor avgjørende at personvernkonsekvenser ved kriminalitetsbekjempelsestiltak vurderes i et helhetlig perspektiv og er gjenstand for offentlig debatt. Utgangspunktet må være at personvern, som en grunnleggende rettighet, må ivaretas også i møte med behovet for effektiv kriminalitetsbekjempelse.

Åpenhet bidrar til å skape tillit. Mangel på informasjon og gjennomsiktighet om teknologibruk, kombinert med en stadig utvikling av kraftige datainnsamlings- og analyseverktøy for bruk i justissektoren, kan føre til svakere personvern. En konsekvens kan bli at befolkningens tillit til justissektoren svekkes. Det er begrenset tilgjengelig informasjon om hvilke verktøy og metoder politiet i Norge anvender, og hvordan personvernet ivaretas i praksis. *Personvernkommisjonen* anbefaler derfor at det nedsettes et utvalg for å utrede metodebruken i justissektoren. Utvalget bør særlig vurdere personvernkonsekvenser av politiets metoder, særlig sett opp mot formålsprinsippet og proporsjonalitetsprinsippet

Det er etter *Personvernkommisjonens* mening avgjørende at systemer og løsninger bygges på en måte som ivaretar personvernet. Dersom lovgiver for eksempel vurderer det slik at omfattende masseinnsamling er avgjørende for bekjempelse av alvorlig kriminalitet, må systemer for lagring av slike data holdes separat fra andre systemer, for å sikre at data ikke kan brukes for andre formål enn innsamlingsformålet.

Videre ser *Personvernkommisjonen* det som avgjørende at Datatilsynet utfører jevnlige kontroller på justisområdet.

Som i andre sektorer, er det også et generelt behov for et kompetanseløft innen personvern i justissektoren. Det innebærer både opplæring av personell, gode rutiner, systemer og verktøy for håndtering av personopplysninger, samt en ledelsesforankret forståelse for personvern som en grunnleggende menneskerettighet. *Personvernkommisjonen* mener det er spesielt viktig at ledelsen i politiet har høy bevissthet om faren for formålsutglidning og at risikoen for slik utglidning reduseres gjennom etablering av gode rutiner og tekniske tiltak. *Personvernkommisjonen* anbefaler også at det etableres bedre systemer for utlevering av dokumenter til advokater, samt at det utredes hvordan opplysninger omfattet av beslagsforbud kan sorteres ut ved gjennomgang av mobiltelefoner.

I *kapittel 8* drøfter *Personvernkommisjonen* hvordan digitaliseringen av skole- og barnehagesektoren har skjedd på bekostning av barns personvern. Skolene og kommunene har i stor grad gjennomført omfattende endringer for å digitalisere skolehverdagen, men har ikke hatt kompetanse og ressurser til å sørge for at personvernet ivaretas som en del av digitaliseringen.

Både lærere, foreldre, elever og skoleledelse tar daglig i bruk et stort antall digitale tjenester som inngår i undervisningen. Svært mange av disse tjenestene, fra læringsmidler til administrative verktøy, behandler store mengder personopplysninger om elevene, som også eksponeres for store mengder reklame, på tross av reklameforbudet i skolen. I mange tilfeller krever det inngående teknologisk og juridisk kunnskap for å ha oversikt over hvordan personopplysninger behandles og brukes i disse systemene, og hvilke personvernkonsekvenser dette kan ha. De fleste kommunene har hverken ressurser eller kompetanse til å gjøre grundige vurderinger på egen hånd, noe som betyr at det i dag er begrenset oversikt over hvordan norske elevers personvern ivaretas. Det er behov for en profesjonalisering og sentralisering av risikovurderinger og testing av digitale løsninger som vurderes brukt i skoler og barnehager.

Personvernkommisjonen anbefaler at det opprettes et nasjonalt kompetanse- og testmiljø for å bistå kommunene med å håndtere personvernutfordringer. Det bør opprettes en nasjonal tjenestekatalog for digitale læringsmidler, som også inneholder personvernvurderinger kommunene og skolene kan ta utgangspunkt i når de skal velge digitale tjenester. I tillegg ønsker *Personvernkommisjonen* at det innføres strakstiltak som kan begrense den kommersiell utnyttelse av elevenes personopplysninger og redusere reklamepresset i tjenestene skolene bruker i undervisningen.

Store globale teknologiselskaper har gjort sitt inntog i klasserommene over hele landet ved å tilby rimelige og brukervennlige tjenester. Den enkelte kommune, skole eller lærer har ikke nødvendig kompetanse, og heller ingen påvirkningseller forhandlingskraft i møte med disse aktørene, og det er derfor stor risiko for at digitaliseringen av skolen skjer på teknologigigantenes premisser. Det er vanskelig å få overblikk over hvordan elevenes personvern ivaretas ved bruk av kommersielle løsninger, samtidig som det kan være problematisk at den enkelte elev får et tidlig forbrukerforhold til selskapene gjennom skolen.

Personvernkommisjonen mener det ikke bør være opp til hver enkelt kommune å forhandle frem avtaler med teknologigiganter, og at nasjonale myndigheter bør komme på banen. Det er også behov for en større debatt om hvilken rolle store teknologiselskaper skal ha i norsk skole. I den grad løsninger som finnes på markedet ikke i tilstrekkelig grad ivaretar personvernet, mener *Personvernkommisjonen* at norske myndigheter må investere i utvikling av nye løsninger som ivaretar personvernet på tilfredsstillende måte.

I *kapittel 9* drøfter *Personvernkommisjonen* utfordringer som er særlig knyttet til forbrukernes personvern, og til bruk av sosiale medier og digitale plattformer i vid forstand. Innsamling og bruk av personopplysninger til kommersielle formål har blitt en sentral del av den digitale forbrukerhverdagen, og har ført til utvikling av en rekke nye tjenester. Utviklingen har også skapt betydelige personvernutfordringer, hvor det i dag er nærmest umulig å unngå at kommersielle aktører samler inn opplysninger om hvem man er, hva man liker og hvor man beveger seg.

Kommersialiseringen av personopplysninger har skapt sterke økonomiske insentiver til å samle inn flest mulig opplysninger. Alt fra hvem man kommuniserer med, hvilke nyheter man leser, hva man kjøper, hvem man elsker og hvor man befinner seg, blir registrert og er gjenstand for analyse og kommersiell utnyttelse. Personopplysninger brukes blant annet til å utvikle nye produkter og tjenester, selges videre, eller brukes til å lage detaljerte profiler som kan anvendes til å målrette atferdsbasert markedsføring og andre budskap.

Utfordringene blir desto større når det dreier seg om kommersiell bruk av barns personopplysninger. Barn har krav på et særskilt vern. Samti-

dig er de flittige brukere av digitale tjenester, og barns personopplysninger samles ofte inn i samme skala som voksnes. Det er umulig å få oversikt over hvordan opplysningene brukes og hvilke fremtidige konsekvenser bruken kan ha. Samtidig har barn rettigheter og krav på vern mot overvåkning, herunder overvåkning utført av egne foreldre. Barnas rettigheter settes under press av digitale produkter og tjenester som lar foreldre følge med på barns bevegelser og aktiviteter. Lovverket som beskytter barn er fragmentert og delvis overlappende, og *Personvernkommisjonen* anbefaler derfor at lovverket gjennomgås og omarbeides for å sikre at barns rettigheter ivaretas.

Personvernkommisjonen anbefaler blant annet at norske myndigheter tar en aktiv rolle opp mot EU når det kommer til forbrukernes personvern, særlig knyttet opp mot pågående lovprosesser. *Personvernkommisjonen* deler Regjeringens syn på at atferdsbasert markedsføring mot barn bør forbys. *Kommisjonen* støtter også at bruken av særlige kategorier av personopplysninger til markedsføringsformål forbys.

Personvernkommisjonen har delt seg i et flertall og et mindretall i spørsmålet om et *generelt forbud* mot atferdsbasert markedsføring bør utredes. *Kommisjonens flertall* mener at det bør utredes hvorvidt et *generelt forbud* er nødvendig for å beskytte norske og europeiske forbrukere. *Kommisjonens mindretall* mener at så lenge atferdsrettet markedsføring gjøres forsvarlig, vil et generelt forbud være uforholdsmessig.

Personvern er i dag ikke et konkurransefortrinn for kommersielle aktører, både fordi det som regel er umulig for forbrukere å ha oversikt over eventuelle personvernkonsekvenser, og fordi det i for liten grad straffer seg å bryte loven. *Personvernkommisjonen* mener at myndighetene har en rolle å spille i å stimulere til utvikling og bruk av personvernvennlig teknologi, både gjennom innkjøpsordninger og anskaffelser, og ved at det slås hardere ned på aktører som ikke ivaretar personvernet. Det er spesielt avgjørende at regelverket håndheves overfor de globale teknologiselskapene, som har en dominerende posisjon i den datadrevne økonomien. Her bør det også vurderes om konkurranselovgivningen kan brukes mer aktivt for å forhindre negative personvernkonsekvenser ved oppkjøp og fusjoner, samt begrense gigantenes markedsmakt for å sikre like spilleregler.

Norge har, som investor, også en unik mulighet til å påvirke globale teknologiselskaper gjennom Statens pensjonsfond utland (Oljefondet), som eier betydelige andeler i teknologigigantene. *Personvernkommisjonen* mener at Oljefondet bør bruke sin investormakt, blant annet ved å utforme personvernkrav som en del av investeringsstrategien. Slik kan mangelfull ivaretakelse av personvernet bli en betydelig investeringsrisiko, som vil kunne skape økonomiske insentiver til å utvikle personvernvennlige løsninger.

1.3.3 Del III – Andre områder kommisjonen har arbeidet med

I *kapittel 10* beskriver *Personvernkommisjonen* den juridiske kompleksiteten i personvernregelverket og drøfter det nasjonale handlingsrommet som følger av forordningen.

Personvernet er regulert av personopplysningsloven og personvernforordningen, som er sektorovergripende regelverk. I tillegg finnes nasjonale, sektorspesifikke regler om behandling av personopplysninger. Forordningen er utformet på en måte som skaper en rekke vanskelige tolkningsvalg. I mange tilfeller forutsetter lovgivningen dessuten at det foretas brede skjønnsmessige avveininger. Ikke sjelden kan det være vanskelig å forstå samspillet mellom personvernforordningen og nasjonal lovgivning. Dette kan skape utfordringer for både de behandlingsansvarlige og de registrerte. *Personvernkommisjonen* anbefaler derfor at det gjøres et kontinuerlig arbeid for å gjøre rettsreglene så forståelige som mulig.

Selv om personvernforordningen i utgangspunktet gjelder likt i alle EU- og EØS-land, er det i bestemte sammenhenger både adgang og plikt til å gi nasjonale regler. I tillegg kan det være behov for nasjonal regulering som bygger bro mellom nasjonal lovgiving og forordningen.

Personvernkommisjonen anbefaler blant annet at regjeringen bør føre en aktiv lovgivingspolitikk for å fremme personvernet, både ved å benytte det nasjonale handlingsrommet, og ved å arbeide aktivt opp mot EU for å styrke felleseuropeisk lovgiving. *Kommisjonen* fremmer også en rekke konkrete forslag til hvordan det nasjonale handlingsrommet kan anvendes.

I *kapittel 11* drøfter *Personvernkommisjonen* hvordan teknologi kan anvendes for å bedre ivareta personvernet. Det handler om hvordan teknologi ikke bare skaper trusler for personvernet, men også kan bidra til å ivareta personvern. Blant annet kan teknologiske verktøy gjøre innbyggerne bedre rustet til å ivareta og anvende sine personvernrettigheter, og til å hjelpe behandlingsansvarlige til å etterleve forpliktelsene de har. *Kommisjonen* beskriver hvordan innebygd person-

vern kan se ut i praksis, gjennom en «rettighetsplattform» hvor innbyggere kan ha tilgang til opplysninger offentlige aktører har om dem, og der de kan få støtte i å utøve rettigheter som for eksempel innsyn, retting og sletting.

Personvernkommisjonen anbefaler at norske myndigheter stimulerer til utviklingen av personvernteknologi, blant annet gjennom innkjøpskrav og økonomiske incentivordninger.

I *kapittel 12* drøfter *kommisjonen* åpenhet som en grunnforutsetning for tilfredsstillende demokratisk deltagelse, personvern og rettssikkerhet.

Personvernet berører flere aspekter ved ytrings- og informasjonsfrihet, og disse rettighetene kan noen ganger komme i konflikt med hverandre. For eksempel kan retten til personvern begrense tilgang til personopplysninger, noe som kan begrense informasjonsfriheten. Samtidig kan personvernet være en viktig forutsetning for at individer velger å ytre seg om kontroversielle temaer. Et godt personvern kan således motvirke nedkjølingseffekter på ytringsklimaet.

Personvernkommisjonen mener det er nødvendig at resultater av automatiserte prosesser som har direkte betydning for innbyggernes plikter, rettigheter, friheter og muligheter, kan forklares. Dersom det for eksempel fattes helt eller delvis automatiserte forvaltningsvedtak, avgjørelse av søknader om lån, eller utmåling av en fengselsstraff, må personer som avgjørelsene gjelder få en forståelig forklaring av hvorfor resultatet fra maskinen ble som det ble.

Åpenhet innebærer også mulighet til å få innsyn i egne personopplysninger, og kunnskap om hvem som har tilgang på disse og hvordan de brukes. *Personvernkommisjonen* mener at det bør være et mål at innbyggerne skal ha tilgang til informasjon om de konkrete registrerte personopplysningene om seg selv. Ved å tilgjengeliggjøre opplysningene trenger ikke den enkelte å måtte søke om innsyn. Det må også legges til rette for at informasjonen er forståelig for de berørte, også for de som mangler grunnleggende digital kompetanse. *Personvernkommisjonen* gir sin tilslutning til viktige konklusjoner i Digitaliseringsdirektoratets utredning av hvordan åpenhet og tilgjengeliggjøring av informasjon om behandling av personopplysninger bør gjennomføres i praksis.

Personvernkommisjonen anbefaler også at de registrerte i større grad bør involveres i utvikling av tjenester. Det er et behov for reell medvirkning i utviklingen av løsninger som behandler personopplysninger.

I *kapittel 13* presenterer *Personvernkommisjonen* Datatilsynets rolle som tilsyn, veiledningsorgan og samfunnsaktør. Datatilsynet har i dag et sektorovergripende ansvar og en betydelig arbeidsmengde, noe som skaper ressursutfordringer ved gjennomføring av lovpålagte oppgaver.

Personvernkommisjonen mener Datatilsynet må styrkes gjennom økte ressurser. Samtidig er det ikke slik at personvernet utelukkende kan sikres gjennom en sterk sentral tilsynsmyndighet. For å styrke personvernet er det nødvendig å sørge for tilgang på personvernkompetanse på alle samfunnsområder, også hos andre offentlige organer enn Datatilsynet.

Fordi personvernregelverket er vanskelig å anvende, er det problematisk at mange behandlingsansvarlige ikke har tilstrekkelig tilgang på veiledning. Dette kan føre til feiltolkning av regelverket og personvernbrudd.

Personvernkommisjonen anbefaler at veiledning av behandlingsansvarlige styrkes. Samtidig bør sektortilsyn i større grad se ivaretakelse av personvern som en oppgave innen sitt arbeidsområde. Dette kan bidra til bedre veiledningstilbud og mer effektiv håndheving.

Kapittel 2
Kommisjonens mandat, sammensetning og arbeid

2.1 Personvernkommisjonens mandat

Personvernkommisjonen ble oppnevnt ved kongelig resolusjon den 23.06.2020.

Kommisjonen ble gitt følgende mandat:

«Regjeringen har i sin politiske plattform (Granavolden-plattformen) bestemt at den vil: «Sette ned en personvernkommisjon for å vurdere personvernets stilling i Norge. Denne skal blant annet se på personvern i justissektoren, og hvordan personvernet kan sikres ved økt bruk av digitale løsninger, herunder rettighetene til brukere av sosiale medier.» Det følger videre av plattformen at «Regjeringen legger til grunn at personvernet er grunnlovsfestet, at enhver har rett til privatliv og at staten har et ansvar for å sikre vern om den personlige integriteten. Presset mot personvernet blir sterkere som følge av økt bruk av digitale løsninger og internett. Regjeringen vil stille strenge krav til sikker lagring og behandling av personopplysninger, både fra private og offentlige aktører.»

Det følger videre av anmodningsvedtak 588 (2017–2018) at: «Stortinget ber regjeringa sjå til at mandatet til den varsla *personvernkommisjonen* inkluderer eit særleg oppdrag om å vurdere stoda for personvernet til barn, og å kome med tiltak for å styrke dette.»

I 2012 startet EU arbeidet med et nytt generelt regelverk om vern av personopplysninger, og i mai 2018 trådte personvernforordningen (GDPR) i kraft i EUs medlemsstater. Forordningen er gjennomført i Norge ved personopplysningsloven 15. juni 2018. Et viktig hensyn i det nye personvernregelverket er harmonisering av regelverket i hele EØS-området, slik at næringsdrivende sikres like vilkår, uavhengig av hvilken medlemsstat de opererer i. Samtidig vil innbyggere i hele EØS-området nyte godt av det samme sterke personvernet, uansett i hvilken medlemsstat de oppholder seg.

I 2014 vedtok Stortinget å styrke vernet om den personlige integriteten ved å ta en bestemmelse om personvern inn i Grunnloven. Retten til privatliv følger også av Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 8 og Europarådets konvensjon om personvern i forbindelse med elektronisk databehandling av personopplysninger ETS nr. 108.

Utfordringsbildet

Norge er et land med høy digital modenhet både i befolkningen og i næringslivet.[1] Digitalisering bidrar til økt velferd, økt produktivitet og økonomisk vekst i så å si alle samfunnssektorer og næringer. Det skapes nye næringer, og forbrukerne endrer vaner og behov i raskt tempo. Digitalisering av tjenester innebærer at det genereres, registreres og behandles langt flere personopplysninger om den enkelte innbygger enn tidligere. Dette er informasjon om geografisk bevegelsesmønster, kontaktnett, helse, økonomi, interesser og andre opplysninger om den enkeltes aktiviteter. Opplysningene kan sammenstilles og analyseres. Det kan bygges profiler om hver enkelt, som kan fortelle svært mye om oss. Også tjenestetilbydere som vi ikke opplever å ha et nært forhold til, kan gjøre denne type analyser av oss, basert på informasjon som deles mellom aktører i den digitale økonomien. Dette har medført et økt press mot personvernet. Samtidig har blant annet innføringen av personvernforordningen bidratt til en betydelig styrking av personvernet på en rekke samfunnsområder.

Personopplysninger samlet inn som følge av økt bruk av digitale tjenester, gir samtidig et unikt potensial for analyse og tjenesteutvikling. Både offentlige og private virksomheter kan bli mer effektive og yte bedre tjenester. Hvor bor de som søker etter informasjon om influensavaksine eller behandling av omgangssyke?

[1] OECD. (2019). *Measuring the Digital Transformation*.

Analyser av slike søk på nett kan hjelpe helsemyndighetene med å forstå befolkningens helsesituasjon raskere og bedre. Datatrafikkanalyser er viktig for at tilbydere av elektronisk kommunikasjon skal kunne planlegge digital infrastruktur som vi er avhengige av. Hver enkelt sjåfør kan, basert på bevegelsene til svært mange biler på samme tid, få anbefalinger om reiseruter som tidligere var umulig å få i sanntid. Transportselskaper kan analysere reisemønstre for å planlegge kapasitet i kollektivtrafikken. Og finansinstitusjoner kan analysere kundenes handlemønstre og bruk av ulike betalingsmidler for å utvikle tjenestetilbudet. Myndighetene kan sette sammen og bruke data til beste for innbyggerne. Personopplysninger kan også brukes til tjenesteutvikling og optimalisering i den enkelte virksomhet, og de har derfor en betydelig markedsverdi.

Potensialet i og presset på kommersiell bruk av personopplysninger er stort. Tjenester tilbys uten brukerbetaling, og baserer seg på videresalg av informasjon om brukerne. Personopplysningenes verdi kan avhenge av hvem som kjøper og selger, og hva opplysningene skal brukes til.

2.1 Gjenbruk av opplysninger til kontrollformål, herunder i justissektoren

Bekjempelse, avdekking, etterforskning og straffeforfølgning av kriminalitet er viktig i en rettsstat. Kriminaliteten endrer seg. Gjerningspersonene tar nye metoder i bruk, også ny teknologi. I mye av justissektorens arbeid er derfor sammenstilling og analyse av elektroniske spor og annen informasjon om innbyggernes aktiviteter, viktig og nyttig. Det er i mange tilfeller gitt adgang til utlevering av informasjon, både mellom organer internt i justissektoren, og mellom justissektoren og forvaltningen for øvrig, for å muliggjøre dette arbeidet.

Samtidig som informasjonsdeling og analyse er viktig for å bekjempe kriminalitet og forhindre overgrep og inngrep i rettssfæren til de som utsettes for kriminalitet, kan det også innebære at personopplysninger brukes til andre formål enn de opprinnelig er innsamlet for. Slik gjenbruk av personopplysninger har økt de siste årene.

Også andre deler av offentlig forvaltning og privat næringsliv gjenbruker stadig oftere personopplysninger til ulike kontrollformål. Toll, skatt og forsikring er eksempler på dette. Personopplysninger gjenbrukes i en del sammenhenger uten at de registrerte er gjort kjent med den aktuelle behandlingen av personopplysninger. I noen sammenhenger er det nødvendig at slik behandling ikke er allment kjent dersom formålet skal oppnås, for eksempel å avdekke skatteunndragelser eller forsikringssvik.

2.2 Personvern i digitale løsninger

Både det offentlige og private benytter i økende grad digitale løsninger. Vi leverer selvangivelsen digitalt, og bruker Altinn for ulike rapporteringer. Vi har bombrikke og elektroniske billetter på buss, bane, båt og fly. Vi bruker nettbank og leser aviser digitalt. Dette, og mange andre gjøremål der det benyttes digitale løsninger, innebærer at vi legger igjen elektroniske spor i en helt annen skala enn ved papirbaserte løsninger.

Offentlige myndigheter ønsker i større grad å sammenstille opplysninger om innbyggerne på tvers av sektorer for å forbedre og effektivisere sine tjenester. Tjenester persontilpasses og automatiseres. Teknologien legger til rette for at opplysninger kan analyseres og benyttes til forskning. Dette legger igjen til rette for gode, offentlige tjenester. Samtidig må hensynet til personvern ivaretas. Sekundærbruk av personopplysninger, f.eks. til forskning, kan ha personvernkonsekvenser. Det er et spørsmål i hvor stor utstrekning myndighetene kan sammenstille, analysere og gjenbruke opplysninger om den enkelte, uten at enkeltindividets tillit til myndighetene påvirkes negativt. Det kan være utfordrende for den enkelte å få informasjon og ha oversikt over behandling av egne personopplysninger. Å lage løsninger som muliggjør utnyttelse av store datamengder, samtidig som det gir færrest mulig personvernulemper for enkeltindivider, er viktig.

Også digitale tjenester i privat sektor forutsetter i varierende grad behandling av personopplysninger. Noen behandler kun høyst nødvendig informasjon for å kunne gjennomføre en avtale, mens andre samler inn data i langt større grad enn nødvendig for å tilby tjenesten. Den digitale forbrukerhverdagen innebærer stadig oftere å måtte gi fra seg personopplysninger for å kunne delta i samfunnet. Fordeler og ulemper ved nye teknologiske løsninger må avveies på en god måte. Samtidig må norske virksomheter være konkurransedyktige i et internasjonalt perspektiv.

I stortingsmeldingen om forbrukerpolitikk, Meld. St. 25 (2018–2019) «Framtidas forbrukar

– Grøn, smart og digital»[2], som ble lagt fram sommeren 2019, ble det identifisert en rekke nye forbrukerutfordringer i den digitale hverdagen. En av utfordringene som omtales i stortingsmeldingen handler om forbrukernes rettigheter, personvern og sikkerhet i digitale produkter og tjenester. Digitale tjenester samler inn store mengder personopplysninger om forbrukerne, noe som forsterkes gjennom utviklingen av tilkoblede produkter i «tingenes internett». Bedrifter benytter personopplysningene til målrettet markedsføring mot forbrukerne.

I 2015 publiserte Datatilsynet utredningen «Det store datakappløpet».[3] I 2020 presenterte Forbrukerrådet en analyse av behandling av personopplysninger i den digitale annonseindustrien.[4]. Rapportene beskriver handel med personbaserte analyser, og hvor lite transparent og, ikke minst, vanskelig dette er å forstå. Analysene brukes til å sende oss reklame og velge ut nyheter som presenteres for oss i nettaviser og i sosiale medier. Reklamen og de utvalgte nyhetene kan påvirke valgene vi tar. Muligheten ikke bare til å påvirke hva vi kjøper, men også – i det skjulte – å påvirke demokratiske prosesser, er betydelig. Skjult påvirkning kan utfordre demokratiet. Det er derfor nødvendig å øke innsikten i, og bevisstheten om, hvordan opplysninger om oss kan brukes til å påvirke de valgene vi tar.

Vi bruker daglig digitale medier til sosial kontakt. I rapporten «Appfail» fra 2016 gjennomgikk Forbrukerrådet 20 apper for å se i hvilken grad forbruker- og personvernrettigheter ble ivaretatt. Tjenestenes bruk av personopplysninger er mer omfattende enn mange er klar over, og gjør det vanskelig å ha kontroll over egne personopplysninger. Informasjon om hvordan forbrukernes personopplysninger blir behandlet er ofte gjemt i lange, kompliserte og, i mange tilfeller, ubalanserte, avtalevilkår.

2.3 Særlig om barns personvern

Grunnloven § 104 gir barn en individuell rett til vern om sin personlige integritet. Barnekonvensjonen artikkel 16 fastslår at barn ikke skal utsettes for vilkårlig eller ulovlig innblanding i sitt privatliv, sin familie, sitt hjem eller sin korrespondanse, eller for ulovlig angrep mot sin ære eller sitt omdømme, og at barnet har rett til lovens beskyttelse mot slik innblanding eller slike angrep. Også personopplysningsloven og personvernforordningen oppstiller særregler for barn, bl.a. inneholder personopplysningsloven § 5 en særlig aldersgrense på 13 år for barns samtykke til bruk av informasjonssamfunnstjenester.

Barnehager og skoler registrerer og lagrer personopplysninger om barn og unge. I tillegg til tradisjonelle opplysninger som orden, oppførsel, atferd, karakterer og utvikling, samles det data gjennom elevenes bruk av nye digitale læringsressurser og skolens kommunikasjon med hjemmet. Dette kan utfordre barn og unges personvern på en ny måte.

Halvparten av avvikene som ble meldt inn til Datatilsynet i 2019 vedrørende barn, skjedde i skolesektoren. Skolene benytter stadig flere typer digitale løsninger. Dette gir ulike personvernutfordringer. Læringsplattformer og nettbrett er en god ressurs i undervisningen, men ved bruken kan det også behandles overskuddsinformasjon, f.eks. stedsinformasjon og informasjon om når leksene ble gjort.

Skolenes bruk av «gratis» applikasjoner i undervisningen medføre at andre får tilgang til omfattende opplysninger om elevene. I praksis har hverken elevene selv eller deres foresatte særlig mulighet til å påvirke innsamling og behandling av personopplysninger ved bruk av slike applikasjoner, og et samtykke til bruk av applikasjonen vil ikke nødvendigvis være reelt.

Barn er aktive brukere av sosiale medier. De kommuniserer selvstendig på sosiale medier fra de er ganske unge. Deling av bilder og video er en naturlig del av barns kommunikasjon. Vi har lite kunnskap om omfanget, og hvordan bruken påvirker barns personvern. Tjenestetilbydere som formidler reklame basert på brukernes informasjon, deling, valg og preferanser, henvender seg også til barn. Slik markedsføring kan være spesielt utfordrende for barn og unge, som har større vanskeligheter enn voksne med å identifisere og forstå reklame. Derfor stiller også markedsføringsloven strenge krav til reklame som er rettet mot barn. Undersøkelser av markedsføring rettet mot barn,[5] viser også at barn blir utsatt for direkte markedsføring som kan være uheldig. Videre har Forbrukerrådet avdekket at internettilkoblede leker og produkter som er rettet mot barn, har vist seg å kunne «overvåke» barnet.

---

2 Meld. St. 25 (2018–2019) *Framtidas forbrukar – grøn, smart og digital*. Barne- og familiedepartementet.

3 Datatilsynet. (2015). *Det store datakappløpet*.

4 Forbrukerrådet. (2020). *Out of control*.

3. Oppdraget

Kommisjonens skal på denne bakgrunn:

- Kartlegge situasjonen for personvern i Norge, og trekke frem de viktigste utfordringene og utviklingstrekkene.
- Kartlegge offentlig sektors behandling av personopplysninger til andre formål enn innsamlingsformålet, og gi en vurdering av de negative personvernkonsekvensene ved dette sett opp mot fordelene.
- Se på utviklingen av personvern i justissektoren og identifisere i hvilken grad det samlede omfanget av tiltak skaper utfordringer for personvernet.
- Kartlegge forbrukeres reelle muligheter til å ivareta eget personvern ved bruk av digitale løsninger og tjenester, og vurdere om bransjenormer, merkeordninger eller sertifiseringsmekanismer kan brukes bedre, jf. personvernforordningen kapittel IV avsnitt 5.
- Utrede hvilke konsekvenser bruk av sosiale medier har for innsamling, analyse og viderebruk av personopplysninger, og foreslå tiltak for å sikre personvernet, herunder den enkelte innbyggers mulighet for å ivareta eget personvern.
- Kartlegge hvordan barn og unges personvern ivaretas i Norge, herunder ivaretakelse av barns personvern i barnehage- og skolesektorene og skolenes bruk av «gratis» applikasjoner der det betales med barns personopplysninger. *Kommisjonen* må i arbeidet se hen til oppfølgingen av NOU 2019: 23 Ny opplæringslov.
- Foreslå tiltak som styrker den digitale forbrukerkompetansen til barn og unge, spesielt knyttet til digital innsamling av personopplysninger og markedsføring i sosiale medier. *Kommisjonen* skal ikke foreslå tiltak som innebærer endringer i læreplanverket Kunnskapsløftet 2020.
- Kartlegge hvordan utstrakt bruk av og eksponering i sosiale medier, herunder brukergenerert innhold, påvirker barn og unges personvern, og foreslå eventuelle tiltak for å bedre personvernet. *Kommisjonen* kan bl.a. kartlegge personvernkonsekvenser ved profilering av barn og se på mulige reguleringer knyttet til bruk av personopplysninger til direktemarkedsføring til barn, samt utrede barns samtykkekompetanse på personvernfeltet.
- Drøfte andre tema som viser seg særlig relevante for å gi et helhetlig bilde på den samlede situasjonen for personvernet I arbeidet skal *kommisjonen* også søke informasjon i våre naboland, og gjøre rede for relevante tiltak som er iverksatt for å ivareta personvernet.»

Personvernkommisjonen skulle opprinnelig levere sin utredning i form av en NOU til Kommunal- og moderniseringsdepartementet innen 1. desember 2021. I brev fra Kommunal- og moderniseringsdepartementet 11. desember 2020 fikk *kommisjonen* forlenget frist til 1. juni 2022. Av hensyn til korrektur og trykkeprosess ble dato for overlevering av utredningen senere satt til 26. september 2022.

2.2 Personvernkommisjonens tolking og avgrensninger av mandatet

Personvernkommisjonens mandat favner vidt. Det har derfor vært nødvendig å gjøre prioriteringer med hensyn til hvilke problemstillinger *kommisjonen* skal gå nærmere inn i. Dette er gjort med utgangspunkt i *kommisjonens* samlede vurdering av utfordringsbildet i lys av det foreliggende kunnskapsgrunnlaget. Dette innebærer at det er problemstillinger og temaer *kommisjonen* ikke har gått nærmere inn på.

Personvernkommisjonen har også foretatt nødvendige avgrensninger av mandatet opp mot andre pågående arbeid og prosesser. Både Ytringsfrihetskommisjonen, Ekspertgruppen for digital læringsanalyse og Medieskadelighetsutvalget har arbeidet delvis parallelt med *Personvernkommisjonen*. I løpet av arbeidet har *Personvernkommisjonen* hatt dialog og møter med disse utvalgene.

Kommisjonen har behandlet personvernutfordringer innen de fire hovedområdene mandatet trekker opp; offentlig sektor/forvaltningen, justissektoren, skole- og barnehagesektoren og forbrukersektoren.

Kommisjonen har tatt utgangspunkt i sentrale drivkrefter og utviklingstrekk som påvirker personvernet, og lagt vekt på teknologi, regelverk, samt generelle samfunnstrekk. *Kommisjonen* har

[5] Rosenberg, T. Grav., Steinnes, K. K., Storm-Mathisen, A. (2018). *Markedsføring og personvern i sosiale medier – en flermetodisk undersøkelse med barn som medforskere*. Forbruksforskingsinstituttet SIFO, OsloMet
Steinnes, K.K., Teigen, H.F. & Bugge, A.B. (2019). *Photophop, fillers og falske glansbilder? En studie blant ungdom om kjønn, kropp og markedsføring i sosiale medier*. Forbruksforskningsinstituttet SIFO, OsloMet.

drøftet personvern som grunnleggende menneskerettighet og vurdert personvernet som en nødvendig rettighet for individer, en viktig kollektiv samfunnsverdi, og en forutsetning for et velfungerende demokrati og rettsstat.

Mandatet fremhever problemstillinger knyttet til offentlig sektors viderebruk av personopplysninger og behandling av personopplysninger til andre formål enn innsamlingsformålet. *Kommisjonen* vektlegger disse utfordringene, men registrerer også andre utfordringer, og har derfor valgt å se bredere på personvernets status i offentlig sektor, blant annet på kompetanse og arbeid med lovgivning. *Personvernkommisjonen* vil gjennomgående i utredningen benytte begrepet *viderebehandling* for å omtale bruken av personopplysninger til et annet formål enn det opprinnelige innsamlingsformålet. Viderebehandlingen kan være forenlig eller uforenlig med innsamlingsformålet, jf. personvernforordningen artikkel 6 nr. 4.

Kommisjonen har avgrenset utredningens kapittel om justissektoren mot sektorer som vekterbransjen og Tolletaten. Behandling av personopplysninger og eksempler fra disse områdene benyttes kun der det belyser situasjonen. Hoveddrøftelsen i kapitlet knyttes til politiet. Det har ikke vært mulig å gå inn i alle ulike spørsmål knyttet til spesifikke politioppgaver, og *kommisjonen* drøfter derfor aktuelle spørsmål på et aggregert nivå.

Mandatet vektlegger barn i flere av punktene. *Personvernkommisjonen* ønsket av denne grunn å involvere barn i *kommisjonens* arbeid og høre deres meninger. For å inkludere barns perspektiv på personvern i utredningen, valgte *kommisjonen* å bestille en ekstern utredning der barn ble intervjuet om sine tanker og kunnskap om temaet.

Kommisjonen mener medvirkningen fra barn i utredningen har gitt et styrket kunnskapsgrunnlag og gitt *kommisjonen* bedre innsikt i hvilke tiltak som vil være relevante og effektive for denne målgruppen. I tillegg er det etter *kommisjonens* syn verdifullt at barn kan få økt innflytelse over samfunnsutviklingen på personvernområdet.

Kommisjonen har valgt å ikke skille ut barns personvern som et eget kapittel, og har i stedet behandlet temaet i henholdsvis kapittel 4 om rettslig regulering, kapittel 8 om personvern i skole og barnehage, og i kapittel 9 om barn som forbruker og i familiære relasjoner.

Mandatet stadfester at *Personvernkommisjonen* skal kartlegge ivaretakelsen av barns personvern i skole- og barnehagesektoren. *Kommisjonen* har avgrenset kartleggingen opp mot arbeidet til Ekspertutvalget for digital læringsanalyse, og har derfor ikke drøftet bruken av verktøy for digital læringsanalyse.

I mandatet pekes det på at *kommisjonen* skal se på forbrukernes reelle mulighet til å ivareta eget personvern ved bruk av digitale løsninger og tjenester. *Kommisjonen* har gjennom sitt arbeid vurdert at forbrukere i dag har svært begrensede muligheter til å ivareta eget personvern, da omfanget av personverninngripende praksis fra kommersielle aktører er meget stort. Derfor har *kommisjonen* valgt å drøfte hvordan forbrukernes personvern settes under press, og hvordan denne utviklingen kan motvirkes gjennom lovgiving, håndheving og endret praksis blant næringsdrivende.

Mandatet sier at *kommisjonen* også skal drøfte andre tema som er særlig relevante for den samlede situasjonen for personvernet. Praktiske tiltak for å beskytte og fremme personvernet forutsetter et effektivt og anvendelig regelverk, samt robuste håndhevings- og veiledningsmekanismer. Derfor har *kommisjonen* valgt å drøfte nasjonalt handlingsrom for lovgivning knyttet til personvernet, og vurdert Datatilsynets virkeområde og rolle som tilsyn og veileder.

Etter *Personvernkommisjonens* syn er åpenhet og praktisk anvendelse av rettigheter hjørnesteiner for ivaretagelse av personvernet. Derfor har *kommisjonen* drøftet hvordan teknologi kan tas i bruk for å fremme personvernet, vurdert tiltak for å fremme åpenhet, samt diskutert individets mulighet for å få utøvet sine rettigheter.

2.3 Kommisjonens sammensetning

Kommisjonen har hatt følgende sammensetning:
- John Arne Moen, konsernsjef, Steinkjer (leder)
- Ingvild Næss, Chief Privacy and Data Trends Officer, Oslo (nestleder)
- Tor-Aksel Busch, pensjonert riksadvokat, Askim
- Trine Skei Grande, direktør bærekraft, Oslo
- Trude Haugli, professor i rettsvitenskap, Tromsø
- Haakon Hertzberg, avdelingsdirektør, Drammen
- Marianne Høyer, nemndleder, Trondheim
- Finn Lützow-Holm Myrstad, fagdirektør, Oslo
- Toril Nag, konserndirektør, Sandnes
- Jill Walker Rettberg, professor i digital kultur, Bergen
- Helge Veum, virksomhetsleder, Ålesund
- Dag Wiese Schartum, professor i forvaltningsinformatikk, Oslo

– Oddhild Aasberg, juridisk seniorrådgiver, Brønnøysund.
– Brita Ytre-Arne, professor i medievitenskap, Bergen

Jill Rettberg fratrådte som kommisjonsmedlem 15. mars 2021.

Brita Ytre-Arne tiltrådte som kommisjonsmedlem 13. juni 2021.

Kommisjonens sekretariat har vært lagt til Kommunal- og distriktsdepartementet, med følgende personer i sekretariatet:
– Hege B. Sæveraas, seniorrådgiver (sekretariatsleder fra juni 2020 til november 2020 og desember 2021 til januar 2022)
– Dana Irina Jaedicke, seniorrådgiver (sekretariatsleder fra desember 2020 til november 2021)
– Catharina Nes, direktør (sekretariatsleder fra og med januar 2022)
– Janne Loen Kummeneje, rådgiver
– Christiane Engelmann Helgar, rådgiver (fra januar 2021 til mars 2022)
– Ailo Krogh Ravna, seniorrådgiver (fra og med februar 2022)

2.4 Kommisjonens arbeid

Første plenumsmøte i *Personvernkommisjonen* ble avholdt 30. september 2020. *Kommisjonen* har totalt hatt 18 plenumsmøter, hvorav 12 to-dagersmøter. På første plenumsmøte valgte *kommisjonen* å dele seg i tre arbeidsgrupper med ansvar for ulike deler av mandatet. Gruppene har avholdt egne møter gjennom hele *kommisjonens* arbeid. Personvernkommisjonen avsluttet sitt arbeid 18. juli 2022. Utredningen er ikke oppdatert med eventuelle regelverksendringer eller andre relevante forhold inntruffet etter denne datoen.

Kommisjonens nettsted (www.personvernkommisjon.no) har vært i drift siden mai 2021 og inneholder blant annet en presentasjon av *Personvernkommisjonens* medlemmer, en side for publikumskontakt, samt en side der dokumenter som *kommisjonen* har publisert har blitt gjort tilgjengelig for publikum. I tillegg har *kommisjonen* avholdt flere innspillsseminar. Det ble gjort opptak av innspillsseminarene, som er publisert på nettsiden. *Personvernkommisjonens* medlemmer har også hatt noe foredragsvirksomhet. Kommisjonsmedlemmene og sekretariatet har deltatt på konferanser, møter og foredrag med relevans for arbeidet.

Kommisjonen har avholdt totalt tre innspillsseminarer om henholdsvis personvern i skolen, teknologitrender og personvern i kommunal sektor.

Følgende personer, organisasjoner og virksomheter holdt innlegg på innspillsseminarene:

Personvern i skolen

– Edvard Botterli Udnæs, Leder i Elevorganisasjonen
– Asle Sandnes, seniorrådgiver, Foreldreutvalget (FUG)
– Kjersti Botnan Larsen, seniorrådgiver, Barneombudet
– Sara Eline Grønvold, spesialrådgiver, Redd Barna
– Line Gaare Paulsen, direktør for kompetanse og samfunnskontakt, IKT Norge
– Simen Sommerfeldt, CTO Bouvet Øst, Bouvet Norge

Teknologitrender

– Tore Tennøe, direktør, Teknologirådet
– Øyvind Husby, administrerende direktør, IKT Norge
– Simen Sommerfeldt, CTO Bouvet Øst, Bouvet Norge
– Erik Lehne, managing partner, Gartner

Personvern i kommunal sektor

– Morten Haug Frøyen, personvernombud, Oslo kommune
– Arnstein Eek, personvernombud, Utsira kommune
– Connie Bjørseth, personvernombud i kommunene Stor-Elvdal, Åmot, Trysil og Engerdal
– Inger Cock-Olsen, personvernombud, Østre Toten kommune
– Harald Torbjørnsen, Foreningen kommunal informasjonssikkerhet (KINS)
– Jan Sandtrø, advokat

Kommisjonen har invitert fagpersoner til å innlede i kommisjonens møter. Dette er:

– Adele Matheson Mestad, direktør for Norges institusjon for menneskerettigheter
– Inga Bejer Engh, barneombud og Kjersti Botnan Larsen, seniorrådgiver, Barneombudet
– Elisabeth Staksrud, professor, Institutt for medier og kommunikasjon, Universitetet i Oslo

- Kristinn Hegna, professor, Institutt for pedagogikk, Universitetet i Oslo
- Leif Ole Topnes, politiinspektør og leder, Felles enhet for utlending og forvaltning (FUF), Kripos
- Rune Reitan, politioverbetjent, Avdeling for Felles Operative Tjenester, Kripos
- Merethe Smith, generalsekretær, og Marius Dietrichson, advokat, Advokatforeningen
- Bjørn Erik Thon, direktør, Datatilsynet
- Åsmund Mæhle, rådgiver og Simen Sommerfeldt, CTO Bouvet Øst, Bouvet Norge
- Anders Lund, seksjonsleder, Sigrid Lian, rådgiver og Aksel Morris Bjørnø, rådgiver, Sikt – Kunnskapssektorens tjenesteleverandør
- Kristine Meek, direktør for kommunikasjon, rådgivning og analyse og Thea Grav Rosenberg, seniorrådgiver kritisk medieforståelse, Medietilsynet
- Asbjørn Tolo, seniorrådgiver, Foreldreutvalget (FUG)
- Christian Sørbye Larsen, prosjektleder SkoleSec, Lene Karin Wiberg, spesialrådgiver, Steinar Hjelset, prosjektmedarbeider SkoleSec og Asbjørn Finstad, avdelingsdirektør Strategisk IKT og digitalisering, SkoleSec, KS
- Runar Karlsen, bransjedirektør for sikkerhet og beredskapsbransjen, NHO Service
- Mona Naomi Lintvedt, stipendiat, Senter for rettsinformatikk, Universitetet i Oslo
- Håkon Hukkelås, stipendiat, NTNU
- Tone Bringedal, seniorrådgiver og Siri Eriksen, Nasjonalt ressurssenter for deling av data
- Fredrik Borgesius, professor, Universitetet i Radboud, Nederland
- Sylvia Peters, fagdirektør, Justis- og beredskapsdepartementet
- Christoph Lutz, førsteamanuensis, Handelshøyskolen BI
- Mareille Kaufmann, professor, Institutt for kriminologi og rettssosiologi, Universitetet i Oslo
- Kjersti Løken Stavrum, leder og Ivar Anders Iversen, sekretariatsleder, Ytringsfrihetskommisjonen
- Marte Blikstad-Balas, leder, Eirin Oda Lauvset, Hilde Hultin og Malcolm Langford, utvalgsmedlemmer, Ekspertutvalget for digital læringsanalyse
- Anja Salzmann, stipendiat ved Institutt for informasjons- og medievitenskap, Universitetet i Bergen
- Janicke Weum, utredningsleder, Christine Hafskjold, fagdirektør og Kristine Regine Buestad Asmaro, seniorrådgiver fra Kommunal- og distriktsdepartementet
- Aasta Margrethe Hetland, seniorrådgiver, Direktoratet for e-helse
- Nils Henrik Heen, juridisk direktør, Finans Norge
- Dag Hareide, forfatter
- Hilde Nagell, rådgiver, Tankesmien Agenda
- Bår Stenvik, forfatter
- Gisle Hannemyr, forsker, Institutt for informatikk, Universitetet i Oslo
- Camilla Nervik, seksjonssjef og Charlotte Bayegan, seniorrådgiver, Datatilsynet
- Suhail Mushtaq, fagsjef, KS
- Fredrik Andersen, leder og Ida Dahl, leder for produkt, Neddy
- Mari Hersoug Nedberg, seksjonsleder personvernseksjonen, Kripos

Kommisjonen har i tillegg fått muntlige og skriftlige innspill til arbeidet fra:

- Avdeling for IT og forvaltningspolitikk, Kommunal- og distriktsdepartementet
- Forandringsfabrikken
- Datatilsynet
- Teknologirådet
- Norsk Lektorlag
- Politidirektoratet
- Kristian Bergem, avdelingsdirektør digitale fellesløsninger, Utdanningsdirektoratet
- Barne- ungdoms- og familiedirektoratet
- Tolletaten
- Statens vegvesen
- Lånekassen
- Helsedirektoratet
- Kompetanse Norge
- Folkehelseinstituttet
- Norsk pasientskadeerstatning
- Nasjonalt organ for kvalitet i utdanningen (NOKUT)
- Digitaliseringsdirektoratet
- KINS
- Arbeids- og velferdsdirektoratet (NAV)
- Utlendingsdirektoratet
- Ola Kristian Hoff, sekretær i Medieskadelighetsutvalget

Kommisjonen vil rette en stor takk til alle bidragsyterne.

Arbeidet under covid-19-pandemien

Kommisjonens arbeid har vært preget av covid-19-pandemien. Som følge av pandemien har mange

møter vært avholdt digitalt. *Kommisjonen* og sekretariatet har lagt ned stor innsats i å opprettholde fremdrift og et godt samarbeid i en krevende tid. De ulike restriksjonene har også medført at *kommisjonen* ikke fikk anledning til å reise på en planlagt studiereise til utlandet.

Kommisjonen har invitert både eksterne forskere og fagfolk, samt utvalgsmedlemmene til å innlede om ulike temaer.

Eksterne utredninger

Kommisjonen har bestilt seks eksterne utredninger:

- «Barns samtykkekompetanse på personvernfeltet», Ingvild Sciøll Ericson. (ligger som digitalt vedlegg til *kommisjonens* utredning)
- «Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering», Mona Naomi Lintvedt. (ligger som digitalt vedlegg til *kommisjonens* utredning)
- «Emerging technologies that can act on human
- body», Gartner.
- «Intervjuer med barn og unge om personvern», Christian Falch.
- «Informasjonsteknologi og personvern. Utviklingstrekk og forslag», Gisle Hannemyr
- «Personopplysninger i skolen», KS

Del I
Hva er personvern, rettslig rammeverk og teknologiske drivkrefter

Kapittel 3
Hva er personvern og hvorfor er det viktig?

3.1 Hva er personvern

Personvern kan defineres og beskrives på ulike måter. Uansett hvilken innfallsvinkel man velger, står det enkelte menneskets ukrenkelighet og krav på respekt fra andre mennesker, virksomheter og myndigheter, respekt for egen integritet og privatlivets fred, sentralt. Personvern er derfor nært knyttet til enkeltindividers muligheter for privatliv, selvbestemmelse og selvutfoldelse. I tillegg kan personvernet sies å være et grunnleggende premiss for et fullverdig demokratisk samfunn.

Prinsippet om individets rett til en privat sfære er forankret i den europeiske menneskerettskonvensjonen[1]: «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse».[2] Personvern er således en grunnleggende rettighet og et fundament mange av de andre menneskerettighetene bygger på. Personvernet er også forankret i Grunnloven: «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet».[3]

I NOU 2009: 1 *Individ og integritet – Personvern i det digitale samfunnet*, redegjorde den forrige *personvernkommisjonen* inngående om personvernbegrepet og utvikling i personverndebatten fra 1970-tallet og frem til begynnelsen av 2000-tallet. *Kommisjonen* viser til redegjørelsen i Del I avsnitt 4 i NOU 2009: 1.[4]

I nyere litteratur forklares personvern som «vern av private sfærer som mennesker befinner seg i».[5] Schartum forstår personvern som en tilstand, en opplevelse av autonomi og integritet innenfor avgrensede områder (private sfærer). Psykisk sfære handler om individets selvfølelse og mentale tilstand. Kroppslig sfære gjelder personens rett til å bestemme over sin egen kropp og friheten fra at andre krenker kroppslig integritet. Geografisk sfære betegner private områder der vi har en forventning om å være i fred og å kunne bestemme selv. Kommunikasjon mellom mennesker bør også kunne skje på en beskyttet måte, som kommunikasjonspartnerne er enige om, og der de er innforstått med hva som er tilgjengelig for hvem.[6] Schartum beskriver også en femte sfære, en «opplysningssfære». Innenfor opplysningssfæren har den enkelte rett til å bestemme over opplysninger om egen person og en mulighet til å justere hvem som skal ha tilgang til disse opplysningene, i tillegg til et krav om at egne valg om dette blir anerkjent og respektert.[7] *Personvernkommisjonen* legger denne forståelse av personvern til grunn, men presiserer at barn og andre individer som ikke har full autonomi og selvbestemmelse også har rett til personvern, blant annet i tilfeller hvor foreldre utøver autonomi på barnets vegne.

Innenfor alle disse sfærene kan det oppstå krenkelser, ved at andre mennesker, virksomheter eller myndigheter, bryter med individenes vernede forventninger til autonomi og integritet. Disse handlingene kan utføres på ulike måter, som ikke nødvendigvis innebærer bruk av teknologi. Innbrudd i noens hjem, «vindustitting», tvungen kroppsvisitasjon og kontroll kan for eksempel krenke personvernet, uten at den som gjennomfører krenkelsen tar i bruk teknologi. Videoovervåkning, profilering, opptak av fingeravtrykk og

---

1 Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4.November 1950 (entered into force 3. september 1953), ETS5, (Menneskerettskonvensjonen).

2 Menneskerettskonvensjonen (EMK) artikkel 8.

3 Lov 17. mai 1814 Kongeriket Norges Grunnlov, (Grunnloven) § 102.

4 NOU 2009: 1 *Individ og integritet – Personvern i det digitale samfunnet*.

5 Schartum, D.W. (2020). *Personvernforordningen: en lærebok*. Fagbokforlaget, s. 13.

6 Schartum, D.W. (2020). *Personvernforordningen: en lærebok*. Fagbokforlaget.

7 Schartum, D.W. (2020). *Personvernforordningen: en lærebok*. Fagbokforlaget.

avlytting, innebærer derimot at individenes handlinger, preferanser eller egenskaper, ved hjelp av teknologi, oversettes til elektroniske opplysninger,[8] som registreres og brukes på en måte som gir mer kunnskap om enkeltpersoner. Digital teknologi skaper muligheter til å generere, samle, og systematisere opplysninger om en persons atferd og væremåte innenfor alle områder en person forventer å kunne opptre «privat». Opplysningene kan brukes som underlag for beslutninger, og kan også påvirke individenes atferd.

3.1.1 Personvern og personopplysningsvern

I juridisk litteratur skilles det gjerne mellom to begreper, *personvern* og *personopplysningsvern*. Personvern kan forstås som vern av den personlige integritet i utvidet forstand. Et vesentlig element i personvernet er at den enkelte skal ha kontroll over, og i størst mulig grad kunne bestemme over egne personopplysninger. Dette innebærer en rett til å få vite hvilke opplysninger andre kjenner til om en selv og hva opplysningene brukes til. Dette omtales ofte som personopplysningsvern, og det er primært denne dimensjonen som er underlagt omfattende lovregulering gjennom blant annet personopplysningsloven, politiregisterloven og regler om taushetsplikt.

Skillet mellom personvern og personopplysningsvern er ikke etablert i dagligtalen. Det er begrepet *personvern* som er innarbeidet, også som uttrykk for det vernet man er berettiget til ved behandling av personopplysninger.

Personvernkommisjonen erkjenner at personvernbegrepet er mangfoldig, og at sammenhengen begrepet brukes i, vil påvirke hvorvidt det dreier seg om personvern i vid forstand eller om det som kan omtales som personopplysningsvern.

Videre i utredningen benytter *kommisjonen* begrepet personvern, også som betegnelse på beskyttelse av personopplysninger.

Personvernkommisjonens arbeid er knyttet til de utfordringene personvernet møter i dagens samfunn. Gjennom mandatet er *kommisjonen* oppfordret til å drøfte hvordan digitaliseringen, og medfølgende økt behandling av personopplysninger, legger press på det grunnlovfestede personvernet.

[8] Tekst, bilder, lyd eller en annen måte å kodifisere informasjon på.

3.2 Ulike elementer i personvernet

Personvern tar sikte på å verne om individer som befinner seg i utvalgte situasjoner, kontekster eller «sfærer». Innenfor den private sfære har individene et ønske og en interesse om å verne deler av sitt liv, sin person og sin væremåte. Det er den enkelte selv som definerer et område der kun de nærmeste slipper inn. Individene må kunne ha en forventning om å kunne definere ikke bare et geografisk/fysisk avgrenset område, men også et mentalt rom der tanker kan være skjermet mot manipulerende og krenkende påvirkning og statlig eller kommersiell kontroll. Personvern kommer også til uttrykk i form av et krav om beskyttet privatliv, skjermet for uønsket oppmerksomhet og forstyrrelser. Med dette kommer en forventning om at definerte grenser, så langt det er mulig, skal respekteres.

Retten til personvern setter også skranker for myndighetenes adgang til å igangsette kontroll og overvåkningsaktiviteter som samler informasjon om hvorvidt folks handlinger er i samsvar med rettslige og sosiale normer. Personvern ivaretar individenes interesse i at kontroller er forholdsmessige. Man bruker ofte begrepene «kontrollsamfunnet» og «overvåkningssamfunnet» for å beskrive samfunn der den enkelte nesten konstant er gjenstand for myndigheters og mektige private aktørers overvåkning og kontroll. En rett til personvern beskytter individene mot maktmisbruk og overdreven kontroll. Både vedvarende overvåkning og mer sporadiske stikkprøvekontroller kan krenke personvernet, dersom de ikke skjer innenfor forutsigbare og kjente rammer.

Selv etter at opplysninger om en selv er tilgjengeliggjort for en mindre eller større krets av personer, består interessen i å bestemme over tilgangen til opplysninger om egen person. Denne idéen er ofte omtalt som «kontekstuelt personvern». Individene er villige til å akseptere en større åpenhet i noen sammenhenger, men kan likevel ha et sterkt ønske om å skjerme seg i andre sammenhenger. Dersom en arbeidsgiver for eksempel registrerer opplysninger om den ansattes seksuelle orientering eller politiske preferanser, kan dette oppleves som krenkende, selv om de samme opplysningene ikke er hemmelige, og er godt kjent for andre man omgås med privat.

Videre er forventningen om at de som «inviteres inn» i ens private rom, og kjenner til informasjon om personlige forhold, ikke misbruker tilliten ved å bruke opplysninger til uventede, uetiske eller ulovlige formål. Å ivareta personvernet er etter dette ensbetydende med å respektere kon-

teksten informasjon er gitt i, intenderte mottakere, og forventninger til mottakernes bruk av opplysningene. Samtidig må det aksepteres at det er flere legitime begrunnelser for å overstyre et slikt individuelt krav om å ikke bruke personopplysningene i strid med forventningene. Flere samfunnsfunksjoner kan ikke ivaretas uten at personopplysninger må behandles. Etterforskning av kriminalitet og straffeforfølgning er typiske legitime innskrenkinger av individenes personvern. Opplysninger behandles som oftest uten individets uttrykkelige samtykke og i praksis vil den enkeltes frie rådighet over egne personopplysninger ofte være kraftig innskrenket.

Personvernet vil i noen tilfeller komme i konflikt med andre rettigheter og samfunnsinteresser. For eksempel kan personvern begrunne begrensninger i ytringsfriheten ved at noen personopplysninger ikke blir offentlige. På den annen side kan nettopp personvern være en forutsetning for ytringsfrihet, for eksempel fordi vern av den enkelte som ytrer seg kan være en forutsetning for at de tør å uttale seg i det offentlige rom. Også på andre måter kan personvern sies å være en forutsetning for andre grunnleggende rettigheter og friheter. Rettssikkerhet forutsetter for eksempel riktig beslutningsgrunnlag. Ofte danner personopplysninger grunnlag for beslutninger, og dersom disse er ulovlig innhentet eller inneholder feil og mangler, vil dette gi dårlig rettssikkerhet.

Hvilken vekt personvernet tillegges i møte med andre interesser er ofte et politisk spørsmål, der ulike aktører forholder seg ulikt, avhengig av prioriteringer, forpliktelser, insentiver og andre faktorer.

3.3 Hvorfor er personvern viktig?

Personvern er en grunnleggende forutsetning i et demokratisk samfunn. Det handler om å beskytte enkeltindivider og grupper, men personvern har også en instrumentell verdi for samfunnet som helhet. Personvern ansees som en individuell rettighet. Denne individuelle rettighetstilnærmingen stammer fra en lang filosofisk og rettslig tradisjon, og er tett sammenbundet med tanken om den liberale rettsstaten. Individets personvern er i mange tilfeller uløselig knyttet til andres personvern, og har således et kollektivt aspekt. Uansett om vi er borgere, forbrukere, eller familiemedlemmer, henger vårt personvern i mange tilfeller uløselig sammen med andres personvern. Et sterkt personvern er derfor både et individuelt gode og et kollektivt samfunnsgode. Disse to perspektivene drøftes kort nedenfor, og legger grunnlaget for videre drøftelser i senere kapitler.

3.3.1 Hvorfor er personvern viktig for individet?

Personvern er en individuell rettighet som legger grunnlaget for privat utfoldelse og meningsdanning. Det gir enkeltindivider og grupper muligheten til å skape og opprettholde private sfærer. Den private sfære kan beskytte oss mot uønskede inngrep ved at vi kan begrense hvem som får tilgang til kroppene, eiendelene og tankene våre og til vår kommunikasjon med andre mennesker. Det bidrar til å skape maktbalanse mellom individet og staten, og individet og private virksomheter.

Den private sfære er en viktig ressurs i et fungerende demokrati. Den er et rom for kritiske tanker, utvikling av holdninger og perspektiver som kan utfordre hva som der og da er alminnelig akseptert – på godt og vondt. Hvis man er redd for å bli overvåket, påvirker det hva som kommuniseres. På denne måten er personvern en forutsetning for retten til ytringsfrihet og tankefrihet.

Et sterkt personvern gir oss muligheter til å mene det vi vil, danne relasjoner med hvem vi vil og være den vi vil være. Det kan være særlig viktig for utsatte grupper og minoriteter, for å verne mot urettmessig overvåkning, diskriminering og maktmisbruk.

Retten til personvern handler dermed om å beskytte den enkelte mot misbruk, ha rom for å handle fritt, til å tenke, føle og være, uten inngripende påvirkning fra myndigheter, virksomheter eller andre. Selv om mennesker har ulike behov for å være private og ulik oppfatning av hva som er privat og ikke, er det grunnleggende at det skal være opp til den enkelte å bestemme når, hvor og hvordan man ønsker å dele eller ikke dele informasjon om seg selv.

3.3.2 Hvorfor er personvern viktig for samfunnet?

I tillegg til å være en grunnleggende individuell rettighet, er personvern også viktig for samfunnet og fellesskapet.

Dersom personvern forstås utelukkede som et individuelt anliggende, kan det være vanskelig å få øye på hvordan den enkeltes personvern også kan påvirke andres personvern. Mange tenker antageligvis at de ikke har noe å skjule, og ivaretakelsen av eget personvern er derfor ikke noe som opptar dem i hverdagen. Denne tankegangen støter på problemer i det sammenkoblede digitali-

serte samfunnet, fordi personopplysninger om en enkeltperson ofte er uløselig knyttet til andre personer. For eksempel vil genetiske opplysninger om deg også gjelde dine barn, og dersom du sender slike opplysninger til et gentestingselskap vil du samtidig ha delt informasjon om barna dine. Dersom et forsikringsselskap tilbyr billigere forsikringspremier til alle som deler helseopplysninger fra en pulsmåler, kan dette føre til at individer som ikke ønsker å la seg overvåke må betale mer. Dermed kan personvernvalg som fremstår som rent individuelle anliggende, ha uforutsette konsekvenser for andre.

Boks 3.1 Tilrettelagt innhenting

Som en del av innføringen av en ny e-tjenestelov, har det vært mye diskusjon om såkalt «tilrettelagt innhenting», tidligere kalt «digitalt grenseforsvar». Solberg-regjeringens forslag om tilrettelagt innhenting gikk ut på at etterretningstjenesten skal ha hjemmel til å samle inn kommunikasjonsdata fra norske internettbrukere som krysser landegrensene. På grunn av hvordan internett er bygget opp, betyr det i utgangspunktet at så godt som all dataflyt krysser grensen, og kritikere har derfor uttalt at forslaget grenser til masseovervåkning.[1] Behovet for tiltaket ble begrunnet med at innhentingen er nødvendig for å avdekke og motvirke trusler mot rikets sikkerhet. Etter at både Sverige og Storbritannia ble felt i Den europeiske menneskerettsdomstolen (EMD) for å ha innført lignende lovendringer, ble bestemmelsen som hjemler anvendelsen av systemet lagt på is.[2] Det er usikkert om tilrettelagt innhenting vil være mulig innenfor rammene som er satt av rettspraksisen fra EMD.

Flere høringsorganer, inkludert Amnesty International, Datatilsynet, Norges Institusjon for Menneskerettigheter, Norsk Presseforbund og Redaktørforeningen har påpekt at tilrettelagt innhenting vil kunne ha alvorlige nedkjølingseffekter, som kan utfordre blant annet ytringsfriheten, kildevernet og konfidensialiteten mellom advokat og klient.[3]

1 Thon. B.E. (2018, 29. november). *Digitalt grenseforsvar, Personvernkommisjon og hva som er godt personvern*. Personvernbloggen. Datatilsynet.

2 Rett 24. (2021, 30. august). *Regjeringen går videre med den kontroversielle delen av e-tjenesteloven*.

3 Forsvarsdepartementet. (2018). *Høring – Forslag til ny lov om Etterretningstjenesten*.

Sammenstilling av opplysninger fra forskjellige kilder betyr også at data om deg kan anvendes på måter som negativt påvirker andre, uten at du selv merker at det skjer. For eksempel kan selskaper som selger ansiktsgjenkjenningsverktøy til undertrykkende regimer ha trent opp systemene sine på bilder hentet fra norske brukere av sosiale medier. Denne typen databruk kan ofte være umulig å forutse for enkeltindivider, og det er utfordrende å stole på at individuelle valg vil begrense slike skadevirkninger.

Det er et grunnleggende problem at det er vanskelig å ta stilling til konsekvenser av egne handlinger som rammer et abstrakt kollektiv, eller som bidrar til skadevirkninger for andre en gang i fremtiden. Det kan dras paralleller til miljø- og klimadiskusjonen, hvor det har vist seg at mange små individuelle valg som virker ubetydelige kan bidra til store samfunnsskader. Dette kalles gjerne allmenningens tragedie.[9]

På tross av at selvbestemmelse er et viktig aspekt ved personvernet, er det svakheter ved å overlate et felles samfunnsgode som personvern til enkeltindividers valg. For eksempel kan valg om hvilken nettleser vi bruker eller hvilke inngrep vi aksepterer, i mange tilfeller være tilsynelatende ubetydelige valg, men hvor de samlede effektene av mange individuelle valg kan påvirke alles personvern. Det understreker viktigheten av å ha demokratisk og regulatorisk kontroll over hvordan personopplysninger samles inn og brukes.

3.3.2.1 Nedkjølingseffekter

Personvernet er en viktig forutsetning for en opplyst og aktiv demokratisk debatt, og for muligheten til å bevege, tenke og ytre seg fritt. Et samfunn der alle kikkes over skulderen til enhver tid, kan gjøre innbyggerne usikre. Et samfunn preget av omfattende overvåkning skaper en såkalt panoptikon-effekt. Begrepet panoptikon stammer fra filosofen Jeremy Bentham, og beskriver et fengselsbygg designet som en sirkel hvor fengselsbetjentene sitter i et tårn i midten med utsikt over hele sirkelen, og fangenes celler er plassert langs sirkelen. Selv om vaktene ikke har kapasitet til å følge med på samtlige fanger til enhver tid, kan ikke fangene vite om de er under oppsyn eller ikke. Dette har en atferdsregulerende effekt – så lenge du vet at du kan være under overvåkning vil du endre oppførsel som om noen ser deg.

9 Laumann, K. & Grytli, D.M. (2021). *Data er det nye oljesølet*. Morgenbladet.

I et samfunnsperspektiv beskrives slike atferdsendringer gjerne som *nedkjølingseffekter*. I Norge har vi for eksempel hemmelig valg og gardiner i stemmelokaler fordi ingen skal kunne påvirke hva du stemmer på valgdagen. Dersom du visste at noen kikket deg over skulderen idet du avla stemmen din, ville dette kunne ha en nedkjølingseffekt som påvirker hvordan du stemte.

I et digitalisert samfunn hvor opplysninger samles inn om nesten alt man foretar seg, risikerer man en overhengende nedkjølingseffekt. Dersom søkemotoren følger med på hva du søker på, kan det for eksempel hende du avstår fra å finne informasjon om en potensielt pinlig sykdom, eller om mulig kontroversielle temaer. Dersom myndigheter har for vide fullmakter til å samle inn personopplysninger, kan det ha alvorlige konsekvenser for blant annet journalistikk, kildevern og i ytterste konsekvens for ytringsfriheten.[10]

I kjølvannet av Snowden-avsløringene, hvor varsleren Edward Snowden avdekket et omfattende overvåkningsnettverk i regi av amerikansk etterretning, observerte forskere at antall Wikipedia-søk på stikkord som kunne føre til muligheter for å havne i myndighetenes søkelys, sank betraktelig.[11] Ifølge forskerne kan årsaken ha vært at bevisstheten om den statlige overvåkningen bidro til at mange vegret seg for å oppsøke slik informasjon. Slike nedkjølingseffekter er særlig problematiske hvis det fører til at borgere ikke tør å oppsøke informasjon som kan være nødvendig for en opplyst samfunnsdebatt – da blir hele samfunnet et panoptikon.

3.3.3 Personvern på tvers av samfunnet

I tråd med digitaliseringen av alle samfunnssektorer har personvern blitt et viktig tema på tvers av samfunnet. Selv om *Personvernkommisjonens* mandat er avgrenset til å særlig vurdere personvern i offentlig forvaltning, justissektoren, skolen og forbrukermarkedet, går de samme utfordringene og problemstillingene, og i mange tilfeller løsningene, igjen i en rekke andre sektorer. Personvernet er en grunnleggende rettighet enten du er pasient, arbeidstaker, flyktning eller pensjonist. Det er ikke lenger tilstrekkelig å vurdere personvern som en arena kun for spesialister og spesielt interesserte – grunnleggende rettigheter må stå sentralt i alle sider av et fritt og demokratisk samfunn.

---

[10] UNESCO. (2015). *World Trends in Freedom of Expression and Media Development: Special Digital Focus 2015.*

[11] Penney, J. (2016). Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal, 31*(1), 117.

Kapittel 4
Rettslig regulering av personvern

Enkeltindividets personverninteresser er ivaretatt gjennom omfattende regulering, både nasjonalt og internasjonalt. Deler av regelverket er utformet som grunntraktater om menneskerettigheter som er nedfelt i kortfattede, generelle bestemmelser. Disse traktatene utgjør det sentrale normative grunnlaget for mesteparten av det øvrige regelverket på feltet, både nasjonalt og internasjonalt.

Personvernkommisjonen vil i dette kapitlet gjennomgå de mest sentrale regelverkene som utgjør det internasjonale rammeverket for beskyttelse av retten til personvern. *Kommisjonen* vil også behandle utvalgte deler av nasjonalt regelverk som er direkte relevant for ivaretakelse av personvern. Politiregisterloven[1] og annen relevant særlovgivning vil bli diskutert i kapitlene som omtaler den aktuelle sektoren. Særlovgivning på helseområdet, herunder pasientjournalloven, helseregisterloven og helseforskningsloven, vil ikke behandles, da helseområdet ikke er en del av *Personvernkommisjonens* mandat.

Kommisjonens mandat inneholder flere punkter der barns personvern er særskilt fremhevet. Av denne grunn vil *kommisjonen* omtale internasjonal og nasjonal lovgivning som berører barns personvern i dette innledende kapitlet. Barns rett til personvern i forbrukersituasjoner og i familiære relasjoner diskuteres i kapittel 9 om forbrukernes personvern.

4.1 Personvern som menneskerettighet

Flere internasjonale traktater om menneskerettigheter anerkjenner personvern som en grunnleggende rettighet. Dette kommer først og fremst til uttrykk i bestemmelser om retten til privatliv («privacy» eller «private life»). Slike internasjonale regelverk har en prinsipiell betydning. Retten til personvern forankres i konvensjoner som tiltres av langt flere stater enn de som har vedtatt spesifikke regler for å verne individer ved behandling av personopplysninger.

Prinsippene som konvensjonene stadfester, er også inntatt i gjeldende lover og regler som omhandler personvern mer direkte. For stater som ikke har tilsvarende regulering av personvern, og ikke er bundet gjennom internasjonale avtaler til å vedta spesifikke regler, kan konvensjonene til en viss grad benyttes for å håndheve en rett til beskyttelse som ellers ikke kan forankres i nasjonal rett. Felles regelverk for beskyttelse av personvern sender også et sterkt signal om at det internasjonale samfunnet anerkjenner og er enige om å slutte seg til felles prinsipper ved behandling av personopplysninger.

Menneskerettigheter kjennetegnes av at de er universelle, ukrenkelige, udelelige og umistelige.[2] Respekt for personvern som en grunnleggende menneskerettighet, innebærer imidlertid ikke direkte plikter for individer og virksomheter. Det er *staten* som gjennom internasjonale avtaler forplikter seg til å ivareta menneskerettighetene. Staten har en plikt til å iverksette lover og regler som beskytter individet, også mot inngrep fra private aktører. Ved å vedta generelle eller særregler som fastsetter plikter for virksomheter som behandler personopplysninger, ivaretar staten sine forpliktelser etter menneskerettighetslovene.

Retten til personvern anerkjennes i FNs Verdenserklæring om menneskerettighetene av 1948[3], artikkel 12,[4] samt i Konvensjon om sivile og politiske rettigheter av 1966 (forkortet «SP»)[5],

[1] Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven).

[2] FN. (2021). *Menneskerettigheter*.

[3] United Nations General Assembly, Universal Declaration of Human Rights, Paris, 10. December 1948 (Menneskerettighetserklæringen).

[4] Artikkel 12 lyder: «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.»

[5] United Nations General Assembly, International Covenant on Civil and Political Rights, 16. desember 1966, Treaty Series, 999, 171. (FN-konvensjonen).

artikkel 17.[6] Konvensjonen er gjort til norsk lov gjennom menneskerettsloven, og bestemmelsene i konvensjonen går foran annen norsk lovgivning ved eventuell motstrid.

Europarådets personvernkonvensjon av 28. januar 1981 er den første og eneste rettslig bindende internasjonale avtalen om personvern.[7] Konvensjonen er ratifisert av Norge, og 52 andre land i verden. Konvensjonen fastsetter en rekke prinsipper, rettigheter og plikter som skal følges ved behandling av personopplysninger, og som partene er forpliktet til å gjennomføre i sin nasjonale lovgivning. I 2018 ble en endringsprotokoll vedtatt og åpnet for signering for både land som er medlemmer av Europarådet og tredjeparter.[8] Endringene sørget for at konvensjonen innholdsmessig er i tråd med personvernforordningen.

EUs charter om grunnleggende rettigheter inneholder også to bestemmelser med særskilt relevans for personvern.[9] Den første er artikkel 7, som gir rett til respekt for privat- og familieliv, hjem og kommunikasjon. Det gis også en særskilt rett i charteret artikkel 8 til «vern av personopplysninger» som del av de grunnleggende menneskerettighetene i EU. Dette innebærer at vern av personopplysninger er ansett som en grunnleggende rettighet. Etter ikrafttredelsen av Lisboa-traktaten[10] i 2009 har EUs charter om grunnleggende rettigheter samme juridiske status som EUs traktater.

4.1.1 Grunnloven

Menneskerettighetene har siden 2014 også fått en sentral plass i Grunnloven. I Grunnlovens § 92 presiseres det at «statens myndigheter skal respektere og sikre menneskerettighetene slik de er nedfelt i denne grunnlov og i for Norge bindende traktater om menneskerettigheter».

Stortinget styrket også vernet om den personlige integriteten i 2014, ved å innta en bestemmelse om personvern i Grunnloven, i § 102:

> «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.»

Etter at personvern ble inntatt eksplisitt i Grunnloven er det usikkert hvilken selvstendig rolle EMK artikkel 8 (se omtale under) vil spille for norsk rett ved beskyttelse av personvern.

Menneskerettighetsutvalget uttalte om samspillet mellom reglene at grunnlovsbestemmelsen:

> «… vil fremheve det rettslige utgangspunkt om ivaretakelse av disse verdiene i norsk rett…», men at «… [d]en nærmere vurderingen eller avveiningen av hvor langt en slik grunnlovsbestemmelse strekker seg, vil måtte forstås i lys av og suppleres med det internasjonale konvensjonsvernet og med tidligere ulovfestet rett.»[11]

Dette innebærer at praksis fra Den europeiske menneskerettsdomstolen (EMD) anses relevant også ved fastleggelsen av grunnlovsbestemmelsene.[12]

Barns rett til personvern er særskilt regulert i Grunnloven § 104 tredje ledd, som slår fast at: «Barn har rett til vern om sin personlige integritet.»[13] Grl. § 104 bygger på sentrale bestemmelser i FNs barnekonvensjon.[14] Konvensjonen gjelder som norsk lov med forrang fremfor annen lovgivning, jf. menneskerettsloven § 3. Barnekonvensjonen omtales nedenfor i avsnitt 4.1.3. Etter Grunnloven § 102 annet ledd skal statens myndigheter sikre et «vern om den personlige integritet». Barns integritetsvern etter § 104 er altså sterkere enn dette. Begrunnelsen for dette er at barn er særlig sårbare, og fordi de i større grad enn myndige personer trenger myndighetenes hjelp for å beskytte sin personlige integritet.

---

6 FN-konvensjonen artikkel 17 lyder omtrent likt som FN-erklæringens artikkel 12 og skal på lik linje med denne beskytte innbyggerne mot inngrep i privatlivet:
«1. Ingen må utsettes for vilkårlige eller ulovlige inngrep i privat- eller familieliv, hjem eller korrespondanse, eller ulovlige inngrep på ære eller omdømme.
2. Enhver har rett til lovens beskyttelse mot slike inngrep eller angrep.»

7 Convention for the Protection of Individuals with regard to the Automatic Prosessing for Personal Data, Strasbourg, 28. januar 1981 (CETS no. 108).

8 Justis- og beredskapsdepartementet. (2018). *Protokoll om endring av Europarådets personvernkonvensjon*.

9 Charter of Fundamental Rights of the European Union, 7. desember 2000 (C 364/01), (Charteret).

10 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, Lisboa, 13. December 2007, (entered into force 1. December 2009), C 306/1, (Lisboa-traktaten).

11 Stortinget. (2011). *Dokument 16 (2011–2012). Rapport til Stortingets presidentskap fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven*, s 175.

12 Heggland, M. (2017). *Barns kontroll over eget personvern gjennom retten til innsyn og samtykke: Styrkes barns rettsstilling ved gjennomføringen av EUs personvernforordning?* [Masteroppgave Universitetet i Oslo]. DUO Vitenarkiv.

13 Grunnloven § 104 ble vedtatt i Stortinget i mai 2014. Før dette var ikke barns rettigheter tematisert i Grunnloven.

14 Convention on the rights of the child, 20. November 1989, (entered into force 2. September 1990) United Nations, Treaty Series, vol 1577, p 3, (Barnekonvensjonen).

4.1.2 Den europeiske menneskerettskonvensjonen artikkel 8

Den europeiske menneskerettskonvensjon av 1950 (forkortet «EMK») ble vedtatt den 4. november 1950 og trådte i kraft den 3. september 1953. Den offisielle norske oversettelsen av artikkel 8 lyder slik:

> «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 rettigheten 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.»

EMK er norsk lov som følge av menneskerettsloven av 1999[15] § 2 nr. 1, og den har forrang foran annen norsk lovgivning ved motstrid, jf. § 3. Det er EMK artikkel 8 andre ledd som har fått størst betydning etter innføring av personvernforordningen. 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.[16]

EMD håndhever konvensjonens bestemmelser i siste instans, herunder artikkel 8. EMD har over tid lagt til grunn at artikkel 8 inkluderer vern av personopplysninger, både for offentlig sektor og privat sektor.[17] I flere saker har EMD drøftet retten til privatliv, og i noen av disse sakene har også vernet ved behandling av personopplysninger blitt satt på spissen.

Beskyttelse av «privatliv» innebærer også en viss grad av beskyttelse av sosiale relasjoner. Barnelovutvalget skriver i sin utredning: «EMK artikkel 8 inneholder også en plikt for myndighetene til å iverksette tiltak – herunder lovgivningstiltak – for å beskytte privatlivs- og familielivsinteresser, til en viss grad også for å beskytte individet mot inngrep i disse interessene som begås av andre privatpersoner. Bestemmelsen har dermed også betydning i forholdet mellom – for eksempel – foreldre og barn.»[18] *Kommisjonen* kommer tilbake til disse problemstillingene i kapittel 9 om forbrukernes personvern.

4.1.3 Barnekonvensjonen og barnets beste

Barn har et selvstendig krav på rett til respekt for sitt privatliv og sitt familieliv etter EMK artikkel 8. Barns rett til personvern er i tillegg gitt særskilt vern gjennom FNs konvensjon om barnets rettigheter (Barnekonvensjonen) artikkel 16.[19] Barnekonvensjonen ble vedtatt 20. november 1989. Den ble bindende for Norge i 1991 og norsk lov i 2003 gjennom et tillegg til menneskerettsloven av 1999.

Barnekonvensjonen setter eksplisitt barnet i sentrum og gir barnet status som selvstendig rettighetshaver. Det følger av konvensjonen at barn har rett til beskyttelse mot «vilkårlig eller ulovlig innblanding i sitt privatliv, sin familie, sitt hjem eller sin korrespondanse, eller for ulovlige angrep mot sin ære eller sitt omdømme.» Barnekonvensjonen artikkel 16 omfatter alle former for krenkelse av den personlige integritet og retten til privatliv, også ved behandling av personopplysninger.

Barnekonvensjonen artikkel 16 skal tolkes i lys av fire generelle prinsipper, som kommer til utrykk i fire ulike artikler i konvensjonen. Disse er artikkel 3 om hensynet til barnets beste, artikkel 12 om retten til å si sin mening og å bli hørt, artikkel 2 om ikke-diskriminering og artikkel 6 om retten til liv og utvikling.

Etter det *Personvernkommisjonen* kjenner til, finnes det svært få avgjørelser å støtte seg til for å klarlegge innholdet i bestemmelsen. Artikkel 16 er imidlertid ansett å omfatte foreldres krenkelse av egne barns personvern, for eksempel hvis foreldre legger ut opplysninger om barnet på internett i strid med barnets rett til privatliv.[20] Bestemmelsen omfatter også innsamling, forvaltning og spredning av personopplysninger om barn.

---

15 Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven).

16 Wiese Schartum, D. & Bygrave, L. A. (2004). *Personvern i informasjonssamfunnet*. Fagbokforlaget. s. 96-97.

17 Se for eksempel *Niemietz v. Tyskland*, [J], no.13710/88, (1992) 16 EHRR 97, og *von Hannover v. Tyskland*, [J] no. 59320/00 ECHR 2004-VI ECHR 294.

18 NOU 2020: 14 *Ny barnelov – Til barnets beste*. s. 65.

19 Convention on the rights of the child, 20. November 1989, (entered into force 2. September 1990) United Nations, Treaty Series, vol 1577, p 3, (Barnekonvensjonen).

20 Bestemmelsen nevnes i en dom fra Høyesterett, HR-2019-2038-A som gjaldt en mors publisering av personopplysninger om sin datter på nett. I dommen legges det til grunn at barnekonvensjonen artikkel 16 gir barn rett til vern om sin personlige integritet.

FNs barnekomité er overvåkingsorgan for barnekonvensjonen.[21] Statene rapporterer om status på overholdelse av Barnekonvensjonens plikter gjennom rapportering hvert femte år til barnekomitéen.[22] Komitéen utarbeider også generelle kommentarer («General comments») om ulike temaer og bestemmelser i konvensjonen. Kommentarene fra barnekomitéen utgjør viktige holdepunkter og retningslinjer for norske myndigheters arbeid med å gjennomføre forpliktelsene etter konvensjonen. Kommentarene er ikke formelt bindende, men har likevel autoritet, idet de bygger på komitéens samlede erfaring og innsikt. Barnekomitéen har utgitt en generell kommentar nr. 25 om barns rettigheter i det digitale miljø, som omtales nærmere i kapittel 9 om forbrukernes personvern.

Barnekonvensjonens tredje tilleggsprotokoll til konvensjonen gir individuell klageadgang for barn. Dette innebærer at barn har mulighet til å klage på behandlingen av egne personopplysninger. Norge har imidlertid ikke tilsluttet seg denne tilleggsprotokollen.[23] Beslutningen har blitt møtt med omfattende kritikk fra Barneombudet.[24]

4.1.3.1 Prinsippet om «barnets beste»

Prinsippet om barnets beste i Barnekonvensjonen artikkel 3 nr. 1 er et av de mest sentrale rettslige prinsippene som omhandler barn. Konvensjonskravet er at barnets beste skal være et grunnleggende hensyn der handlinger «berører barn». Begrepet «grunnleggende hensyn» i artikkel 3 nr. 1 viser til at hensynet til barnets beste ikke bare er et av flere momenter i en helhetsvurdering, men et hensyn som skal ha stor vekt. At det skal være et grunnleggende hensyn, medfører likevel ikke at barnets beste alltid trumfer andre hensyn. Det skal komme frem av begrunnelsen at barnets beste er vurdert, samt hvordan dette hensynet er avveid mot andre hensyn som gjør seg gjeldende.[25] Dersom motstridende hensyn har like stor vekt som hensynet til barnets beste, vil imidlertid sistnevnte trumfe i avveiningen.[26]

I vurderingen av hva som er barnets beste, er det også relevant å legge vekt på foreldrenes synspunkter. Dette er særlig aktuelt der det er tvil om hva som er det beste for barnet. Barns rett til å bli hørt er også helt grunnleggende. Det er nær sammenheng mellom prinsippet om barnets beste og retten til å bli hørt.[27]

Hva som vil være til det beste for det enkelte barn i en konkret situasjon, beror på en individuell og konkret vurdering, men når det gjelder behandling av personopplysninger må det kunne legges til grunn et slags føre-var-prinsipp. Det vil være bedre å opptre med varsomhet slik at ikke personopplysninger havner på avveie eller lignende. Det faktum at barns personopplysninger typisk kan volde problemer for barnet i fremtiden, er også et eksempel på dette. Prinsippet om barnets beste behandles også i kapittel 9 om forbrukernes personvern.

4.2 Personopplysningsloven og personvernforordningen (GDPR)

4.2.1 Personvernforordningen

Personvernforordningen[28] inneholder bestemmelser om behandling av personopplysninger innen de fleste samfunnsområder, og er det personvernregelverket med klart størst praktisk betydning. Forordningen gjelder imidlertid ikke behandling av personopplysninger for rent private og familiemessige aktiviteter. Opplysninger som brukes «innenfor husets fire vegger» faller derfor utenfor, men ikke dersom opplysningene legges åpent ut på for eksempel sosiale medier. For justissektoren (for eksempel politi og domstoler) gjelder det dessuten egne regler i politidirektivet[29], som primært er gjennomført i norsk rett i politiregisterloven.

Personvernforordningen gjelder direkte i alle land i EØS, og inneholder de aller fleste bestemmelser om hvordan personopplysninger skal

---

21 Barnekonvensjonen artikkel 43 flg.

22 FNs barnekomité åpner også for supplerende informasjon fra ikke-statlige aktører som nasjonale overvåkingsorgan og organisasjoner fra sivilt samfunn. Barneombudet er en av aktørene som sender slike supplerende rapporter. Se Barneombudets rapporter her: Om barnekonvensjonen og rapportering – Barneombudet.

23 Manglende praksis fra komitéen, og lite kunnskap om hvordan klageordningen ville fungere, ble tillagt stor vekt i avgjørelsen om ikke å tilslutte seg tredje tilleggsprotokoll. konvensjon_barn.pdf (regjeringen.no).

24 Barneombudet. (2017). *Barneombudets supplerende rapport til FNs barnekomité: Barns rettigheter i Norge – 2017.*

25 Committee on the Rights of the Children, General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1), pkt.III, 14b.

26 Committee on the Rights of the Children, General comment No. 14 (2013 pkt. 39).

27 Committee on the Rights of the Children, General comment No. 14 (2013 pkt 43).

28 Forordning (EU) 2016/679) om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning).

behandles. Personvernforordningen gjelder i utgangspunktet likt, «ord for ord», i alle EØS-land. Ambisjonen om felles regler er imidlertid ikke gjennomført fullt ut. I forordningen finnes mer enn 30 bestemmelser som gjelder nasjonal regulering. Det nasjonale handlingsrommet, og hvordan dette kan og bør brukes, diskuteres nærmere i kapittel 10 om regelverkskompleksitet og nasjonalt handlingsrom.

Den norske personopplysningsloven[30] har primært tre funksjoner. For det første bestemmer den at personvernforordningen skal gjelde som norsk lov og ved konflikt gå foran annen norsk lov. For det andre inneholder den en rekke bestemmelser som bare gjelder i Norge. Dette betyr at en alltid må ta utgangspunkt i personvernforordningen, og sjekke om det er gitt særregler for Norge i personopplysningsloven. Norske særregler kan imidlertid også finnes i annen norsk lovgivning. For det tredje inneholder personopplysningsloven bestemmelser om de norske myndighetene på området: Datatilsynet og Personvernnemda.

Personvernforordningen inneholder mange bestemmelser, men det er de fem første kapitlene som har størst betydning for det løpende arbeidet med vern av personopplysninger. Den andre halvdelen av teksten gjelder i stor grad tilsynsmyndighetenes oppgaver og myndighet, håndhevelse og sanksjoner, og adgangen til å fastsette nasjonal lovgivning på enkelte, sentrale saksområder

De aller fleste bestemmelsene i personvernforordningen er generelle og forutsetter ikke en bestemt type behandling. Likevel er det gitt enkelte særlige bestemmelser om profilering, helt automatiserte avgjørelser, og direkte markedsføring. I personopplysningsloven er det i tillegg gitt regler om forbud mot kameraovervåking eller andre handlinger som gir inntrykk av at kameraovervåking finner sted.[31]

4.2.2 Hva gjelder personvernforordningen for?

Personvernforordningen gjelder for «behandling av personopplysninger». Personopplysninger er alle opplysninger som *kan knyttes til en fysisk person*. Det er altså nok at det vil være mulig å kople en opplysning til en person; det trenger ikke å ha skjedd. Når en bil kjører gjennom en bomstasjon, er det normalt ingen som finner ut hvem som sitter i bilen, men fordi det er *mulig* å gjøre det, er registreringen av bilen en personopplysning. De aller fleste bestemmelsene i personvernforordningen gjelder alle opplysninger, uansett om de ikke oppfattes som spesielt sensitive i dagliglivet. I tillegg gjelder strengere bestemmelser for særlige kategorier personopplysninger, inkludert opplysninger om etnisitet, religion, politisk oppfatning, helseopplysninger, seksuell legning og flere andre opplysningstyper som en generelt anser som spesielt sensitive.

Personopplysninger kan fremkomme på en rekke måter, blant annet som skrift, foto, video, tegning, lyd, eller registering i sensor. «Behandling» dekker alt en kan gjøre med en personopplysning, inkludert innsamling, strukturering, prøving av vilkår, beregning, videresending, lagring, og all annen bruk. Til sammen gjør dette at «behandling av personopplysninger» angir et veldig omfattende saklig virkeområde for personvernforordningen. Forordningen forutsetter stort sett at behandlingen er automatisert. Det er nok med delvis automatisering for at forordningen skal gjelde. Er behandlingen helt automatisert, gjelder det egne strenge regler. Forordningen gjelder også for manuelle personregistre, altså strukturerte manuelle samlinger av personopplysninger.

4.2.3 Hvem gjelder personvernforordningen for?

Personvernforordningen inneholder primært regler som «behandlingsansvarlige» virksomheter og enkeltpersoner må følge. Grovt sagt vil alle som samler inn personopplysninger om andre bli regnet som behandlingsansvarlige. For eksempel vil en kommune være behandlingsansvarlig når den samler inn opplysninger om elever i grunnskolen, eller en konsertarrangør vil være behandlingsansvarlig når den registrerer hvem som kjøper billetter til en konsert. Den behandlingsansvarlige er den som fastsetter formålet med behandlingen av personopplysninger og bestemmer hvilke hjelpemidler (for eksempel IT-systemer) som skal benyttes. I virksomheter er det den øverste ledelsen for virksomheten som har behandlingsansvaret. Det er egne regler for tilfeller der to eller flere behandlingsansvarlige samarbeider.

Behandlingsansvarlige kan inngå avtale med andre virksomheter om at de skal behandle personopplysninger på den behandlingsansvarliges vegne. Slike virksomheter kalles *databehandlere*,

---

29 Direktiv (EU) 2016/680 om beskyttelse av fysiske personer ved behandling av personopplysninger for å forebygge, etterforske, avdekke eller straffeforfølge lovbrudd eller gjennomføring av straffereaksjoner, og om fri utveksling av slike opplysninger og opphevelse av rådets rammebeslutning 2008/977/JIS.

30 Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).

31 Jf. personopplysningsloven § 31.

og skal være underlagt en egen avtale og behandlingsansvarliges instruksjonsmyndighet.

Personvernforordningen er tuftet på *ansvarsprinsippet*, som innebærer at den behandlingsansvarlige har ansvar for at personvernprinsippene og enkeltbestemmelser i forordningen ellers etterleves. Dersom dette ikke skjer, kan den behandlingsansvarlige (eventuelt databehandler) bli ilagt store overtredelsesgebyrer, og eventuelt bli idømt erstatningsplikt.

Personvernforordningen gir personer det er registrert opplysninger om (de «registrerte») en rekke rettigheter overfor den behandlingsansvarlige. Blant annet kan registrerte personer kreve innsyn i egne personopplysninger. Den behandlingsansvarlige har i tillegg plikt til å på eget initiativ gi registrerte en rekke opplysninger om hva og hvordan personopplysningene om de registrerte blir behandlet. Den enkelte registrerte kan også be om at opplysninger rettes, suppleres eller slettes, protestere mot at spesielt belastende opplysninger om dem blir behandlet, eller motsette seg helt automatisert behandling av personopplysninger. Den behandlingsansvarlige skal legge til rette for bruk av rettigheter, eventuelt ved å lage systemløsninger som gjør det lettere å bruke dem (for eksempel innsynsrutiner, rutiner for å gi og trekke tilbake samtykke).

Personvernforordningen inneholder også en rekke bestemmelser om hvordan de nasjonale tilsynsmyndighetene skal samarbeide, herunder om Det europeiske personvernrådet (EDPB) og dets oppgaver og myndighet. Samlet utgjør de nasjonale tilsynene og rådet et felles europeisk tilsynsapparat som skal sikre effektiv og lik praktisering av forordningen i hele EØS. Samarbeidsmekanismene mellom tilsynsmyndigheter beskrives nærmere i kapittel 13.

Enkelte bestemmelser i personvernforordningen gjelder nasjonale lovgivere, og fastsetter regler for når det skal eller kan gis nasjonale bestemmelser, og de nærmere krav til slike bestemmelser. Områdene ytringsfrihet, innsyn i offentlige saksdokumenter og personvern i arbeidstakerforhold er eksempler på områder med et visst nasjonalt handlingsrom. I kapittel 10 behandles nasjonalt handlingsrom nærmere.

4.2.4 Hvor gjelder personvernforordningen?

Personvernforordningen er basert på at personopplysninger skal kunne flyte fritt i EØS. Verneni-

Boks 4.1 Schrems II

Den 16. juli 2020 kom den såkalte «Schrems II»-dommen. EU-domstolen vurderte om Facebook brøt reglene i personvernforordningen i forbindelse med at Facebook overførte personopplysninger om europeiske brukere til USA. Dommen har betydning for all overføring av personopplysninger fra land i EU til land utenfor EU.

For det første kom EU-domstolen frem til at Privacy Shield var et ugyldig overføringsgrunnlag. Begrunnelsen var at USAs overvåkningspraksis og regelverk strider mot flere av reglene i personvernforordningen og EU-charteret. Konsekvensen er at Privacy Shield ikke kan benyttes som overføringsgrunnlag.

For det andre la domstolen til grunn at standard personvernbestemmelser (SCCs) ikke uten videre er et gyldig overføringsgrunnlag. I noen tilfeller, for eksempel ved overføring av personopplysninger til USA, vil det være nødvendig å implementere ytterligere beskyttelsestiltak som er egnet til å avhjelpe risikoene som følger med et utilstrekkelig beskyttelsesnivå i landet man overfører personopplysninger til.

Tiltakene som iverksettes kan være organisatoriske, tekniske eller juridiske. Eksempler på organisatoriske tiltak kan være streng tilgangskontroll, ulike kontraktsforpliktelser kan brukes som et juridisk tiltak og kryptering og pseudonymisering er eksempel på tekniske tiltak. For virksomhetene kan det være komplisert og krevende å vurdere hva som vil være et tilstrekkelig beskyttelsesnivå og hvilke tiltak som bør iverksettes. Personvernrådet (EDPB) har gitt ut en veiledning om Schrems II og hva denne dommen betyr for overføring av personopplysninger.[1] Datatilsynet har også utarbeidet en veiledning om overføring av personopplysninger til tredjeland.[2]

[1] European Data Protection Board. (2020). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.*

[2] Datatilsynet. (2021). *Overføring av personopplysninger ut av EØS.*

våret anses å være likt uansett hvor i EØS behandlingen skjer, og lovligheten skal kun bedømmes ut fra de felles reglene. Personvernforordningen gjelder all behandling av personopplysninger i regi av virksomheter og enkeltpersoner som er *etablert i EØS*. Hvis en norsk virksomhet er etablert i Norge, og dels behandler personopplysninger i Norge og flere andre land i og utenfor EØS, gjelder forordningen likt i alle disse landene. Alle enkeltpersoner det er samlet opplysninger om, har de samme rettighetene.

Forordningen gjelder for behandlingsansvarlige som er etablert *utenfor EØS* når de tilbyr varer og tjenester til personer som oppholder seg i EØS. På samme måte gjelder forordningen dersom behandlingsansvarlige utenfor EØS følger med på atferden til enkeltpersoner i EØS, for eksempel hvordan de bruker nettbaserte tjenester.

For overføring til land *utenfor EØS* gjelder egne bestemmelser som skal sikre tilstrekkelig personvern når personopplysninger blir overført til USA, Kina og andre land som ikke har samme vernenivå som i EØS. Således inneholder forordningen flere alternative fremgangsmåter for å gjøre overføring til tredjeland. Forordningen kan likevel være et reelt hinder for at overføring til tredjeland kan skje.

4.2.5 Personvernprinsippene

De fleste bestemmelsene i personvernforordningen inneholder vanlige rettsregler. I tillegg er det formulert seks *personvernprinsipper*, se artikkel 5 nr 1. Prinsippene er en slags grunn-normer for behandling av personopplysninger, og gir generelle retningslinjer for hva en skal legge vekt på for å ivareta personvernet. Prinsippene er utviklet over en periode på mer enn 40 år, og har lenge ligget til grunn for ulik europeisk personvernlovgivning. De er alltid relevante og alltid obligatoriske å ta hensyn til.

Prinsippet om *lovlighet, rettferdighet og åpenhet*, innebærer blant annet krav om at behandling av personopplysninger skal være i samsvar med personvernforordningen, og med annen EU-lovgivning og internasjonale menneskerettigheter. En konsekvens er blant annet at personvern må vurderes opp mot andre grunnleggende rettigheter og friheter, for eksempel ytringsfrihet og diskrimineringsvern. Rettferdighetskravet innebærer blant annet at motstående interesser skal veies mot hverandre på forholdsmessig, lyttende måte, uten forutinntatte meninger. Prinsippet markerer også at åpenhet er en grunnforutsetning for personvern. Åpenhet er både en forutsetning for at folk skal kunne beskytte og bruke rettighetene sine, og for at det skal være mulig for tilsynsmyndighetene og andre å bedømme om reglene blir etterlevet.

Formålsbegrensningsprinsippet innebærer at en før personopplysninger blir samlet inn, må bestemme seg for hva opplysninger skal brukes til, og i utgangspunktet holde seg til disse formålene. I avsnitt 4.2.7 blir reglene om formål nærmere gjennomgått. Nevnte behandlingsformål spiller en helt sentral rolle for forståelsen av flere av de andre prinsippene, fordi formålet er referanseramme for andre vurderinger.

Dataminimeringsprinsippet innebærer at en ikke må behandle flere opplysninger enn det formålet gjør nødvendig, og at opplysninger ikke må brukes i større utstrekning enn nødvendig.

Riktighetsprinsippet innebærer krav om at personopplysninger skal være så riktige og fullstendige som formålet tilsier.

På lignende måte uttrykker *lagringsbegrensningsprinsippet* at personopplysninger ikke skal lagres over lenger tid enn formålet tilsier.

Prinsippet om integritet og konfidensialitet innebærer informasjonssikkerhet og ivaretakelse av opplysningenes integritet, tilgjengelighet og konfidensialitet. På grunn av dette prinsippet, er sikring av personopplysninger et tungtveiende hensyn ut over de konkrete reglene om sikkerhet i artikkel 32 – 34 av forordningen.

4.2.6 Behandlingsformål og behandlingsgrunnlag

Reglene i personvernforordningen må i stor grad etterleves *før* den behandlingsansvarlige har samlet inn personopplysninger. Når behandling av opplysninger skjer automatisk, betyr det at IT-systemer og andre løsninger som skal benyttes må være utformet slik at de sikrer etterlevelse av bestemmelsene i forordningen.

Formålsbegrensningsprinsippet nevnt over uttrykker ikke bare et prinsipp, men er også en rettsregel om at det ikke er anledning til å samle inn personopplysninger uten at ett eller flere behandlingsformål er fastsatt slik forordningen krever. Disse formålene må dessuten være knyttet til et *behandlingsgrunnlag*, det vil si en hjemmel som gjør det lovlig å behandle personopplysninger. Samtykke er et eksempel på et slikt mulig behandlingsgrunnlag. Ofte trenger den behandlingsansvarlige imidlertid ikke å innhente samtykke, men kan påberope seg at det er nødvendig å behandle personopplysningene for grunner som er angitt i forordningen. For eksempel kan man

behandle opplysninger som er nødvendige for å inngå eller gjennomføre en avtale med den registrerte (for eksempel en avtale om kjøp på nettet). Nedenfor gjør *Personvernkommisjonen* nærmere rede for flere andre viktige behandlingsgrunnlag. Dersom behandlingsansvarlige ønsker å behandle særlige kategorier personopplysninger,[32] må det være et eget behandlingsgrunnlag for disse, i tillegg til de alminnelige kravene til behandlingsgrunnlag.

4.2.6.1 Behandling av barns personopplysninger

Utgangspunktet etter personvernforordningen er at barn og voksne har samme rettigheter når det gjelder behandling av personopplysninger. Dette betyr at alle reglene i personvernforordningen også gjelder for barn. Forordningen inneholder enkelte spredte artikler og fortalepunkter om behandling av barns personopplysninger, men gir ingen samlet enhetlig regulering av temaet. Forordningen inneholder heller ingen definisjon av hvem som skal regnes som barn i forordningens forstand. Ved innføringen av personvernforordningen antok imidlertid Justis- og beredskapsdepartementet at en person ikke lenger er et barn i forordningens forstand når vedkommende har fylt 18 år.[33] Departementet viste også til at dette utgangspunktet er i overensstemmelse med utgangspunktet i FNs konvensjon 20. november 1989 om barnets rettigheter artikkel 1 som gjelder som norsk rett, jf. menneskerettsloven § 2 nr. 4.[34]

Ved behandling av personopplysninger om barn, plikter den behandlingsansvarlige å informere om hvilke legitime interesser som forfølges ved behandlingen, og formålene med behandlingen, jf. personvernforordningen artikkel 13 nr. 1 bokstav d og artikkel 14 nr. 1 bokstav c. Denne informasjonen skal gis på «*en kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk, især når det gjelder informasjon som spesifikt er rettet mot et barn*» jf. artikkel 12 nr. 1.

Fortalepunkt 58 presiserer at «*ettersom barn fortjener et særlig vern, bør all informasjon og kommunikasjon, dersom behandlingen gjelder barn, være formulert på et klart og enkelt språk som barnet lett kan forstå*».

Det er naturlig å forvente at både den legitime interessen som taler for behandlingen og konsekvensene behandlingen kan ha for barns personvernrettigheter (eller andre rettigheter og friheter), fremgår uttrykkelig av informasjonen den ansvarlige publiserer (for eksempel i personvernerklæringer).

Det er usikkerhet knyttet til hvor stor vekt det skal tillegges at den registrerte er et barn. Det vil bero på en konkret vurdering i hver enkelt sak. Når den behandlingsansvarlige vurderer at deres legitime interesse er mer tungtveiende enn barns rettigheter og friheter og igangsetter behandlingen, så bør den behandlingsansvarlige synliggjøre begrunnelsen for å sette hensynet til barns personvern til side. Ofte vurderer behandlingsansvarlige at ordinære informasjonssikkerhetstiltak iverksatt i forbindelse med behandlingen er tilstrekkelig for å ivareta barns personvern. En slik vurdering vil ikke være i tråd med regelverket. Det må i tillegg foretas en prinsipiell vurdering av om behandlingen i det hele tatt burde igangsettes overfor barn.

4.2.7 Betydningen av risikovurderinger

Et viktig kjennetegn ved sentrale deler av personvernforordningen er kravet til å vurdere risiko, og til å vurdere hvilke tiltak som kan settes inn for å redusere risikoen til et akseptabelt nivå. Perspektivet for den behandlingsansvarlige er altså: Hva kan skje/gå galt som setter folks personvern og andre grunnleggende friheter og rettigheter i fare, og hva kan jeg gjøre for å forhindre dette? Denne tilnærmingen følges i bestemmelsene som fastsetter behandlingsansvarliges krav til å sikre etterlevelse av forordningen, kravene til personopplysningssikkerhet, og kravene til personvernkonsekvensvurderinger (DPIA[35]). Personvernforordningen stiller klare krav til personvernkonsekvensvurderinger.

Vilkårene for å gjennomføre en vurdering av personvernkonsekvenser er at det er «sannsynlig» at behandlingen vil medføre «høy risiko for fysiske personers rettigheter og friheter», jf. personvernforordningen artikkel 35 nr. 1. Dersom det er tilfellet, må det gjennomføres en personvernkonsekvensvurdering i tråd med reglene i artikkel 35 før behandlingen av personopplysningene starter. I sannsynlighetsvurderingen skal det

---

[32] Opplysninger om etnisitet, religion, politisk oppfatning, helseopplysninger, seksuell legning og flere andre opplysningstyper som en generelt anser som spesielt sensitive.

[33] Prop. 56 LS (2017–2018) *Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen*, kap 13.2.1.

[34] Prop. 56 LS (2017–2018).

[35] «Data Protection Impact Assessment», se personvernforordningen art. 35 nr. 1.

blant annet tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i.

Den risikobaserte tilnærmingen får også anvendelse i forbindelse med lovgivningsprosesser, herunder prosesser som innebærer utarbeidelse av nye eller endring av eksisterende forskrifter. For å avgjøre om en ny lov eller forskrift innebærer en høy risiko for personvernet, må det nødvendigvis gjennomføres en risikovurdering. Se nærmere om vurderinger av personvernkonsekvenser i lovarbeid i kapittel 6.

Risikovurderinger står også sentralt i kravet til å bygge personvernprinsippene inn i teknologi og organisering, for eksempel krav om innebygd personvern, som omtales i kapittel 11.

Personvernforordningen innebærer ikke krav til fravær av risiko, men krever at den behandlingsansvarlige skjønnsmessig bedømmer hva som er *akseptabel* risiko. Det betyr blant annet at jo større og mer alvorlige mulighetene for krenkelse av personvernet er, desto mer må den behandlingsansvarlige gjøre for å redusere sannsynligheten for og følgene av at det uønskede skjer.

Den behandlingsansvarlige skal iverksette tiltak som er nødvendige for at risikoen skal bli akseptabel. Tiltakene kan for eksempel være tekniske, organisatoriske, juridiske, pedagogiske eller økonomiske. Ethvert tiltak som kan være virksomt og hensiktsmessig skal vurderes.

4.2.8 Dokumentasjonsplikter

Behandlingsansvarlige og databehandlere som har flere enn 250 ansatte, har grunnleggende forpliktelser til å dokumentere behandlingen av personopplysninger i *behandlingsprotokoller*. Protokollene skal være tilgjengelige for tilsynsmyndighetene.

Alle behandlingsansvarlige plikter også å rapportere til tilsynsmyndigheten om sikkerhetsbrudd som sannsynligvis gir risiko for rettighetene og frihetene til individer det er registrert opplysninger om.

I tillegg har behandlingsansvarlige en plikt til å kunne *påvise* at behandlingen av personopplysninger skjer i samsvar med reglene i forordningen. Muligheter for å bli ilagt overtredelsesgebyr og idømt erstatningsplikt kan også gjøre at behandlingsansvarlige ønsker å «dokumentere sin uskyld», altså vise at det er vist aktsomhet, vurdert risikoer og truffet forsvarlige tiltak.

De ovenfor nevnte forholdene kan gjøre at behandlingsansvarlige og databehandlere ønsker å dokumentere eller på annen måte beskrive hva som faktisk er gjort, men det er ingen faste krav til slik dokumentasjon. Flere bestemmelser i forordningen gir for eksempel rett til innsyn i, eller plikt til å gi informasjon om, «relevant informasjon om den underliggende logikken …» av helt automatiserte avgjørelser og profilering.[36] Dette medfører i utgangspunktet ingen plikt til å ha en skriftlig, tilgjengelig forklaring som kan brukes for å etterleve bestemmelsene. Dette drøftes videre i kapittel 12 om åpenhet.

4.2.9 Virkemidler for å ivareta personvernet

Retten til personvern er som nevnt nedfelt i internasjonale, rettslig bindende traktater, forordninger, direktiver, samt nasjonal lovgivning. Lovgivning gir i utgangspunktet et sterkt vern, men personvernlovgivningen alene vil ikke kunne gi individene reell beskyttelse. Mange av bestemmelsene på personvernområdet er vage og flertydige, slik at de kan være vanskelige å omsette til organisatoriske rutiner eller tekniske løsninger. For å gi individene tilstrekkelig vern, er det derfor avgjørende at lovens krav tolkes og virkeliggjøres gjennom teknologiske, organisatoriske, økonomiske eller pedagogiske virkemidler.

Til denne utredningens formål er det ikke mulig eller hensiktsmessig å legge frem en uttømmende liste over strategier og verktøy for å ivareta personvernet. Ulike tiltak er iverksatt i ulike sektorer, gjerne i kombinasjon med hverandre.

Hvilke typer virkemidler som bør benyttes, vil avhenge av typen av personopplysninger og hvem som behandler personopplysninger. Noen virkemidler kan iverksettes av behandlingsansvarlige og databehandler selv. Andre nødvendiggjør mer omfattende endringer og involverer lovgivere, tilsyn eller kontrollmyndigheter.

Teknologiske virkemidler, herunder innebygd personvern omtales i kapittel 11.

Organisatoriske virkemidler kan for eksempel være ulike atferds- og bransjenormer, sertifiseringer og personvernombud. Personvernombudsrollen behandles i kapitlene 6, 7 og 13.

Atferds- og bransjenormer er et sett med regler eller retningslinjer som spesifikt regulerer en bransje. Slike normer er frivillige for aktører i bransjen å underskrive. I personvernforordningen er det lagt opp til at bransjer kan lage egne bransjenormer som kan godkjennes av Datatilsynet.[37] Det er lagt til rette for at slike atferdsnormer kan få gyldighet i EU.[21] Brudd på normene vil ikke i

[36] Se personvernforordningen art. 15 nr. 1 bokstav h.

[37] Personvernforordningen art. 40.

seg selv kunne føre til offentligrettslige reaksjoner.[38]

Sertifisering er en formalisert form for evaluering som skal lede til utstedelse av et sertifikat.[39] Hensikten med en sertifisering eller en merkeordning er å få en bekreftelse på at for eksempel en gjenstand møter visse standarder eller et IKT-system møter en satt standard for personvern.

Målet med sertifisering eller merkeordning er å vise at behandlingsansvarlig eller databehandler overholder kravene personvernforordningen stiller knyttet til den spesifikke behandlingen som sertifiseres. Bakgrunnen for sertifiseringer er at det gjør det enklere for forbrukere og eventuelle samarbeidspartnere å kjenne igjen aktører som følger forordningen.

I tillegg til de foran nevnte virkemidler, finnes økonomiske virkemidler som for eksempel incentivordninger, budsjettpolitikk og pedagogiske virkemidler som holdningskampanjer.

Tilsyn og håndhevelse av regelverket diskuteres i kapittel 13.

4.3 Relevante kommende regelverk

Personvernforordningen er bygget på prinsippet om et felles lovverk i Europa, og EU-domstolens avgjørelser er med på å forme rettstilstanden og påvirker tolkingen av forordningen.

Personvernkommisjonen vil i det følgende kort gjøre rede for kommende regulering av digitale markeder, kommunikasjonsvernforordningen, forslag til forordning for kunstig intelligens, samt Dataforordningen og Datastyringsforordningen. De kommende regelverkene søker å videreføre målsetningen om å skape et helhetlig lovverk innad i unionen, som også er forutberegnelig og tar hensyn til bruk av personopplysninger på tvers av landegrenser.

Kommunikasjonsvernforordningen

I januar 2017 offentliggjorde Europakommisjonen et forslag til kommunikasjonsvernforordningen (e-privacy regulation) som skal erstatte det nevnte kommunikasjonsverndirektivet.[40] Målet med forslaget til forordningen er å sikre et effektivt og godt vern av konfidensialitet for elektronisk kommunikasjon, og å oppdatere reglene i tråd med den teknologiske utviklingen.[41]

Kommunikasjonsvernforordningen omhandler behandling av personopplysninger og overlapper dermed med personvernforordningens virkeområde. Kommunikasjonsvernforordningen vil bli lex-specialis opp mot personvernforordningen, og bestemmelsene i kommunikasjonsvernforordningen vil dermed få forrang ved motstrid.[42]

Europakommisjonen hadde som mål at forordningen skulle tre i kraft samtidig som personvernforordningen. Kommunikasjonsvernforordningen er imidlertid i juli 2022 ennå ikke vedtatt. Grunnen til dette er blant annet at det har vært vanskelig for medlemslandene å enes om et mandat.[43] I januar 2021 ble medlemmene i Rådet likevel enige om et forhandlingsmandat.[44] I følge dette forhandlingsmandatet vil forordningen omfatte elektronisk kommunikasjonsinnhold som sendes via offentlige tilgjengelige tjenester og nettverk, og metadata tilknyttet denne kommunikasjonen, som sted, tidspunkt og mottaker. Regelverket skal tre inn når sluttbruker befinner seg i EU, men omfatter også tilfeller hvor behandlingen finner sted utenfor EU, eller hvor tjenestetilbyderen er etablert eller befinner seg utenfor EU. Regelverket vil omfatte datakommunikasjon mellom maskiner (tingenes internett) som sendes via et offentlig nettverk. Rådet forhandler videre om mandatet med Europakommisjonen og Europaparlamentet.

Forordning om digitale tjenester (Digital Services Act)

Forordningen om digitale tjenester (Digital Services Act, DSA) er foreløpig på forslagsstadiet. DSA skal bidra til større demokratisk kontroll og tilsyn med internettbaserte tjenester og plattformer, sikre like markedsvilkår for plattformtilbyderne, redusere risiko for manipulasjon og desinformasjon, og bidra til å motvirke ulovlig innhold på nett. DSA gir regler om markedsplasser (for eksempel nettbutikker), sosiale plattformer, platt-

---

38 Prop. 56 LS (2017–2018), side 118.

39 Hofstad, K. (2022). *Sertifisering*. Store norske leksikon.

40 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussel, 10. januar 2017, COM (2017) 010 final.

41 EØS-notatbasen. (2021). *Forslag til kommunikasjonsvernforordning*.

42 Lex specialis gir spesielle regler fortrinn fremfor mer generelle regler. Dette innebærer at et unntak vil ha fortrinnsrett fremfor en hovedregel.

43 Stortinget. (2021, 17. februar). *Rådets enighet om ePrivacy åpner for datalagring*.

44 Rådet for den Europeiske Union. (2021, 10. februar). *Confidentiality of electronic communications: Council agrees its position on ePrivacy rules.*

former som deler innhold, appstores og online reise- og hotellplattformer. Forordningsforslaget oppdaterer også deler av gjeldende e-handelsdirektiv. Forordningsforslaget omtales nærmere i kapittel 9 om forbrukernes personvern.

Forordning om digitale markeder (Digital Markets Act)

Forordningen om digitale markeder (Digital Markets Act, DMA) ble godkjent av Rådet den 18. juli 2022. DMA regnes som den mest betydningsfulle reguleringen av det digitale markedet siden personvernforordningen.

DMA skal bidra til en mer åpen og rettferdig plattformøkonomi, og skal gjennom en konkurranserettslig forhåndsregulering hindre atferd som er skadelig for konkurransen og forbrukerne fra de største plattformene. Forordningen skal sikre konkurransen og åpenheten mellom digitale plattformer, gi brukerne flere og bedre tjenester å velge mellom, større muligheter til å bytte plattformleverandør og bedre priser. Forordningen om digitale markeder omtales nærmere i kapittel 9 om forbrukernes personvern.

Forslag til forordning for kunstig intelligens

EU arbeider for tiden med en ny forordning for å regulere kunstig intelligens (KI). Forordningen forventes å tre i kraft i perioden mellom 2022 og 2024. Forordningen har blant annet som mål å styrke tilliten til kunstig intelligens ved å stille krav om og legge til rette for en ansvarlig bruk av kunstig intelligens som ivaretar europeiske verdier og rettigheter.[45]

Regelverket skal i følge Europakommisjonen ikke berøre personvernforordningen, men være et supplement til personvernregelverket.[46] Forslaget til forordning for kunstig intelligens blir omtalt nærmere i kapittel 9 om forbrukernes personvern.

Datastyringsforordningen (Data Governance Act)

Datastyringsforordningen ble lagt frem av Europakommisjonen 25. november 2020 og er per juli 2022 til behandling i Rådet og i Europaparlamentet.

Europakommisjonens forordningsforslag tar sikte på å skape en sikker infrastruktur for datadeling, og et indre marked for deling av ikke-personlige data (industrielle data). Dette skal gjøre det mulig for data å bevege seg fritt innen EU og EØS, på tvers av sektorer. Målet er å styrke den digitale suvereniteten på dataområdet ved å etablere en europeisk datahåndteringsmodell, som en motvekt til de store plattformselskapene.

Forordningsforslaget skal skape grunnlaget for en europeisk datastyringsmodell som er i overensstemmelse med EUs prinsipper og verdier, som personvern, forbrukerbeskyttelse og konkurranseregler. Det nye regelverket etablerer et juridisk rammeverk for ni sektorspesifikke europeiske dataområder: helse, industri, landbruk, finans, mobilitet, klima, energi, offentlig administrasjon og ferdigheter. Dette skal blant annet bidra til bedre energistyring, skreddersydde legemidler og enklere tilgang til offentlige tjenester. Datastyringsforordningen tilrettelegger også for såkalt «data-altruisme», som skal gjøre det lettere for virksomheter og personer å gjøre sine data tilgjengelig til det beste for samfunnet. Forslaget inneholder regler for nøytrale datatilbydere som skal fungere som et sikkert mellomledd ved datadeling, men ingen krav til datalokalisering (plikt til å lagre og behandle data i EU).

Dataforordningen (Data Act)

Europakommisjonen la 23. februar 2022 fram et forslag til forordning om harmoniserende regler om rettferdig tilgang til og bruk av data (dataforordningen).[47] Forslaget fra Europakommisjonen skal drøftes i Rådet og Europaparlamentet, og det kan bli justeringer i det materielle innholdet i løpet av denne prosessen.

Forslaget gir regler om å fremme deling av data som er av samfunnsinteresse, fremme datadeling innad i næringslivet, klargjøre regelverket for ansvarlig bruk av data og legge til rette for frivillig datadeling som grunnprinsipp.

---

45 Europakommisjonen. (2022). *Regulatory framework proposal on artificial intelligence*.

46 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, Brussel, 21. april 2021 COM (2021) 206 final, se avsnitt 21.2

47 Forslag til europaparlaments- og rådsforordning om europeisk datastyring (Data Governance Act) på Europakommisjonens hjemmesider.

Kapittel 5
Det teknologiske landskapet som påvirker personvernet

Vi lever i en epoke som kan beskrives som informasjonsalderen. Den gjennomgående digitaliseringen av så godt som alle samfunnssektorer drives i stor grad frem av nye muligheter for innsamling, registrering, transport og bruk av informasjon i form av data. I dette kapitlet vil *Personvernkommisjonen* kort redegjøre for de antatt viktigste teknologiske utviklingstrekkene som har betydning for personvernet. Kapitlet er ikke ment å gi en komplett oversikt, men vil gjøre rede for noen viktige grunnleggende teknologiområder.

Den følgende teksten er delvis basert på en rapport skrevet av Gisle Hannemyr på oppdrag fra *Personvernkommisjonen*. *Kommisjonen* vil også drøfte samspillet mellom teknologisk og samfunnsmessig utvikling, samt noen samfunnsmessige konsekvenser av en utvikling som ikke ivaretar personvernet. Der særlige teknologier eller teknologianvendelser er grunnleggende problematiske for personvernet, særlig knyttet opp mot ansiktsgjenkjenning og annen biometrisk fjernidentifisering i offentlige rom, vil *kommisjonen* vurdere om regulering eller forbud er hensiktsmessig. Konkrete praktiske eksempler på teknologianvendelser i ulike samfunnssektorer vil presenteres i nærmere detalj i påfølgende kapitler, der det er relevant.

5.1 Teknologiske utviklingstrekk med betydning for personvernet

Det er en overordnet politisk målsetning at alle samfunnssektorer skal digitaliseres.[1] Digitaliseringen bidrar til stor grad av effektivisering og verdiskaping i både offentlig og privat sektor ved at komplekse oppgaver kan automatiseres, tjenester kan integreres med hverandre og sentraliseres, og informasjon kan flyte mellom tjenester. Det kan skape store gevinster på viktige områder som helsesektoren, forbrukertjenester og offentlig forvaltning.

Digitaliseringen betyr at samfunnet blir datadrevet. Når en tjeneste digitaliseres, innebærer det at opplysninger blir registrert og omgjort til data, enten det gjelder industrielle data fra maskiner eller helseopplysninger om innbyggerne. Når opplysninger er omgjort til data kan de som regel sammenstilles, gjenbrukes og foredles i det uendelige.

I 2022 koster datalagring mindre enn en tidel av hva det gjorde for ti år siden, og skytjenester gjør at man kan få enkel og billig tilgang til lagring og regnekapasitet. De fallende prisene gjør det mulig å lagre enorme mengder data og med nye metoder kan de store datamengdene sammenstilles for å finne skjulte sammenhenger og atferdsmønstre, en prosess omtalt som stordata-analyse.

Dagens informasjonsalder er muliggjort av fire sentrale drivere som *kommisjonen* vil komme tilbake til i dette og senere kapitler:

- Sporingsteknologier og sensorer tilrettelegger for økt innsamling av data.
- Nye infrastrukturer for tilkobling (for eksempel 5 G) tilrettelegger for mer effektiv transport og overføring av data.
- Lagringsteknologi (for eksempel skytjenester) muliggjør lagring av store mengder data.
- Kraftig prosesseringskraft muliggjør automatisk analyse av enorme datasett, blant annet gjennom maskinlæringssystemer.

Disse fire drivkreftene er tett sammenbundet. I dette kapitlet vil kommisjonen beskrive noen konkrete teknologianvendelser aktualisert av disse driverne og hvordan de kan utfordre personvernet.

5.1.1 En digital hverdag

Norge er et av verdens mest digitaliserte land, og digitaliseringen har blitt en integrert del av så godt som alle samfunnsområder. For eksempel har om lag 96 prosent av alle nordmenn smarttele-

[1] Se for eksempel Meld. St. 27 (2015–2016) *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet.* Kommunal- og distriktsdepartementet.

fon.[2] Det betyr at nesten alle nordmenn er digitalt tilkoblet stort sett overalt og hele tiden. Alt fra varehandel, trening, kontakt med det offentlige, helseverktøy, offentlig diskusjon, mediebruk og banktjenester foregår helt eller delvis gjennom telefonen. Covid-19 pandemien akselererte digitaliseringen av blant annet arbeidslivet og utdanningssektoren, og understreket samfunnets avhengighet av teknologiske verktøy for å kommunisere, formidle og søke informasjon, samt for å handle varer og tjenester.

Det er enorme muligheter knyttet til digitaliseringen av samfunnet, men det intensiverer også bruken av folks opplysninger i en helt annen skala enn tidligere. Fremover vil beslutningstagere i stadig større grad måtte håndtere juridiske og etiske dilemmaer, der potensialet for betydelig samfunnsgevinst må veies opp mot grunnleggende personvernhensyn.

5.1.1.1 Digitalt utenforskap

Selv om de fleste nordmenn har et aktivt forhold til digitaliseringen gjennom deltagelse på digitale plattformer, bruk av datamaskiner og smarttelefoner, samt at stadig større deler av forvaltningen og møte med offentlige myndigheter digitaliseres, har ikke utviklingen ivaretatt alle deler av befolkningen i samme grad. Det anslås at det er om lag 600 000 nordmenn som mangler grunnleggende digital kompetanse av forskjellige årsaker.[3] Dette har skapt et digitalt utenforskap som lager nye skiller i samfunnet. I kapittel 12 diskuteres digitalt utenforskap og hvordan det kan påvirke muligheten til selvbestemmelse i det digitale samfunnet.

5.1.2 Teknologiske fundamenter for det digitale samfunnet

Som beskrevet ovenfor, har teknologiutviklingen muliggjort automatisk innsamling og behandling av store mengder data, såkalt stordata-analyse. Prosesser og fenomener som tidligere var rent fysiske blir registrert som datapunkter, og virkeligheten blir på denne måten formalisert, datafisert og kvantifisert.[4]

Utviklingen medfører at personopplysninger som er samlet inn kan viderebehandles til flere forskjellige formål. Som nærmere beskrevet i kapittel 6, opererer for eksempel offentlig forvaltning med et «kun én gang»-prinsipp, hvor opplysninger som samles inn om innbyggere som en del av forvaltningsprosesser skal kunne viderebehandles av andre etater, slik at innbyggere ikke bes om å oppgi de samme opplysningene flere ganger.

Digitaliseringen henger tett sammen med globaliseringen av stadig flere områder, både som en driver og som en effekt. Digitale infrastrukturer er som regel grensekryssende, og muliggjør informasjonsflyt uavhengig av geografisk lokasjon. De største teknologiaktørene opererer på et globalt nivå, og setter premisser for datainnsamling og behandling på tvers av landegrenser.

5.1.2.1 Sporingsteknologi og sensorer

Den allestedsnærværende databehandlingen som preger informasjonsalderen, muliggjøres av forskjellige teknologier som registrerer virkeligheten ved å omgjøre fysiske fenomener til kvantifiserbare og lesbare data. Slike teknologier omfatter *sensorer* og *sporingsteknologier*.

Sensorer registrerer opplysninger om det fysiske rom i sanntid og inkluderer bevegelsessensorer, kameraer som automatisk analyserer omgivelser, mikrofoner, og mye mer. Sporingsteknologier inkluderer sensorer som registrerer data om en person eller gruppe over tid, slik som sporingsbrikker, samt programvare som samler inn opplysninger, for eksempel sporingskapsler (coo-

Boks 5.1 Sporingsteknologi på nett

De fleste er vant til å få forespørsler om å godta informasjonskapsler, eller cookies, når de beveger seg rundt på nett. Dette er små tekstfiler som lagres i nettleseren, og som tilrettelegger for å lagre informasjon om brukerens preferanser og atferd. Informasjonskapsler er imidlertid kun én av mange teknologier som benyttes til å samle inn informasjon om forbrukere på nettsider eller i apper. Blant annet kan informasjon om skjermstørrelse kombinert med operativsystem og annen metadata brukes til å lage unike «fingeravtrykk» for å spore brukere. De fleste smarttelefoner kommer også med unike ID-numre som brukes til å samle inn og sammenkoble informasjon om brukerne.

2 Statistisk Sentralbyrå. (2021). *Norsk mediebarometer*.

3 Kompetanse Norge. (2021). *Befolkningens digitale kompetanse og deltakelse*.

4 Mejias, U. A. & Couldry, N. (2019). Datafication. *Internet Policy Review 8*(4).

kies) på nettsider eller sporingspiksler i eposter.[5] Varianter av slik teknologi finnes overalt, for eksempel i biler og kollektiv trafikk, på nettsider, i smarttelefoner, integrert i smarthusløsninger, i helseutstyr og på kjøpesentre. Sensorer kan blant annet erstatte eller forsterke menneskelige sanseapparat, for eksempel ved å forbedre syn gjennom avanserte kameraer, hjelpe personer med nedsatt synsevne ved å identifisere skrift, og mye mer. Det krever imidlertid nye analyseverktøy for å kunne analysere og bearbeide all informasjonen som samles inn.

5.1.2.2 Maskinlæring og stordata

Teknologiutviklingen innenfor sporingsteknologi og sensorer muliggjør innsamling av betydelige mengder data, men det er umulig for mennesker å håndtere informasjonsmengden – det krever automatisering. Selv om lagring og aggregering av informasjon ikke er et nytt fenomen, er det først ved utviklingen av kraftige datasystemer at potensialet i store mengder data kan hentes ut. Ved hjelp av *maskinlæringssystemer* kan betydelige mengder opplysninger struktureres og analyseres, og blant annet brukes til å finne nye sammenhenger og utlede prediksjoner, gjerne kalt «prediktiv analyse». Prediktiv analyse fungerer ved at et maskinlæringssystem analyserer historiske data for å identifisere mønstre, som brukes til å forutse sannsynligheten for at en hendelse vil inntreffe i fremtiden.

Maskinlæringssystemer er en betegnelse for datasystemer som «lærer» og endrer atferd av seg selv for å finne mønstre i store datamengder ved bruk av statistiske metoder, uten at et menneske må formulere regler for hvordan informasjon skal behandles.[6] Maskinlæringssystemer består av avanserte algoritmer, matematiske modeller som beskriver fremgangsmåten for løsning av en oppgave. Gjennom å kunne operere uten betydelig menneskelig innblanding, kan systemer basert på maskinlæringsalgoritmer utføre stadig mer komplekse oppgaver. Likevel er maskinlæringsmodellene laget av mennesker, og utviklerne av systemene setter premisser for blant annet hvordan læringen skal foregå og hvilke treningsdata som brukes i opplæringen. Maskinlæringssystemer som er selvgående ved at de kan operere uten betydelig menneskelig innblanding, kalles gjerne kunstig intelligens.[7]

Boks 5.2 Datainnbrudd mot Norkart

I mai 2022 ble selskapet Norkart, som leverer IT-systemer for kart- og eiendomsinformasjon, utsatt for et dataangrep. Som et resultat av angrepet havnet personopplysninger om opp mot 3,3 millioner huseiere på avveie. I etterkant av datainnbruddet advarte flere eksperter om at opplysningene kan misbrukes av svindlere for å manipulere potensielle ofre, eller til identitetstyveri.[1]

[1] NRK. (2022, 11. mai). *Advarer mot skreddersydd svindel etter datalekkasje.*

I dagligtalen brukes ofte begrepene «maskinlæring», «algoritme» og «kunstig intelligens» om hverandre, særlig når det er snakk om selvlærende datasystemer som anvendes til å automatisere prosesser, forutse hendelser og/ eller produsere anbefalinger. *Personvernkommisjonen* bruker begrepet «maskinlæringssystemer» gjennomgående i denne utredningen.

5.1.3 Samfunnssikkerhet i et digitalt samfunn

Digitaliseringen av samfunnet har ført til betydelige endringer i samfunnssikkerhetsbildet på tvers av landegrenser og nasjonalt. Den store mengden informasjon som samles inn og analyseres av vidt forskjellige aktører, bidrar til et bredt og uoversiktlig risiko- og trusselbilde for både myndigheter, virksomheter og individer. Det kan inkludere at fremmede statlige aktører eller kriminelle får tilgang til samfunnskritisk infrastruktur, som for eksempel ved hacking av et kraftverk, eller at sensitive opplysninger havner på avveie på grunn av et datainnbrudd. Utviklingen fører til at sikkerhetsmyndighetene må være årvåkne i møte med stadig nye trusler, hvor nye sårbarheter i infrastruktur eller programvare kan dukke opp over natten. På et individuelt nivå skaper informasjonsinnsamlingen risiko for identitetstyveri og andre former for svindel, samt større og mer tilgjengelige former for både statlig og kommersiell overvåkning.

[5] Datatilsynet. (2015). *Det store datakappløpet.*

[6] Tidemann, A. & Elster, A. C. (2022). *Maskinlæring.* Store norske leksikon.

[7] Teknologirådet. (2018). *Kunstig intelligens – muligheter, utfordringer og en plan for Norge.*

Datainnbrudd er et stadig økende problem, hvor næringssensitive eller personsensitive opplysninger havner på avveie med potensielt alvorlige følger. Det betyr at alle aktører som samler inn, behandler og deler personopplysninger må gjøre grundige sikkerhets- og personvernvurderinger før de samler inn og lagrer data, og i tillegg iverksette både organisatoriske og tekniske tiltak.[8]

5.1.3.1 Omfattende kommersiell sporing skaper sikkerhetsutfordringer

Den kraftige veksten av kommersiell sporing har muliggjort nye forretningsmodeller basert på innsamling, bruk og salg av personopplysninger, som av kritikere blir kalt *overvåkningsøkonomien* eller *overvåkningskapitalismen*.[9] Det finnes en rekke kommersielle aktører som samler inn opplysninger på tvers av tjenester for å kartlegge forbrukere, og som deler og selger informasjonen til et bredt spekter av forskjellige tredjeparter. Denne utviklingen beskrives nærmere i kapittel 9 om forbrukernes personvern.

Spredningen av personopplysninger har bidratt til et uoversiktlig risikobilde. Det er mangel på kontroll med hvem som har tilgang på personopplysninger og hvem de deler og selger opplysningene til. Dette skaper fare for misbruk fra både kriminelle og fremmede makter. Man kan også se for seg at store kommersielle aktører blir kjøpt av selskap i land med omfattende nasjonal overvåkning. Tilgang på store mengder personopplysninger kan for eksempel brukes til påvirkningsoperasjoner, utpressing og overvåkningsformål, og kan således utgjøre en alvorlig trussel for det nasjonale sikkerhetsbildet.[10]

5.1.3.2 Sikkerhetstiltak som legger press på personvernet

Sikkerhet og personvern er ikke i utgangspunktet motpoler eller motstridende interesser, og godt personvern er i mange tilfeller et viktig sikkerhetstiltak. Likevel vil det i en rekke situasjoner måtte gjøres avveininger mellom sikkerhet og retten til personvern. Som beskrevet i kapittel 7, er dette ofte en problemstilling i justissektoren. Offentlig debatt om samfunnssikkerhetshensyn sett opp mot retten til personvern har blant annet tilspisset seg i diskusjoner rundt datalagringsdirektivet og det såkalte digitale grenseforsvaret.[11] I disse tilfellene har ønsker om å forhindre kriminalitet eller trusler fra fremmede makter måtte veies opp mot borgernes rett til personvern. Et stadig mer komplisert digitalt trusselbilde gjør at avveiningen må tas i stadig flere tilfeller.

Avveininger mellom informasjonssikkerhet og personvern er også en utfordring innenfor blant annet arbeidsliv og helsesektoren, hvor et økende trusselnivå for datainnbrudd og lignende cyberangrep kan føre til økt ønske eller behov for mer overvåkning, for eksempel gjennom logging, kameraovervåkning og systemer for identifikasjon for å hindre uautorisert adgang til fysiske eller digitale rom. Slik overvåkning kan styrke sikkerheten, og være viktig for å hindre datainnbrudd og dermed i realiteten ivareta personvernet til kunder av en virksomhet. Samtidig legger overvåkning press på personvernet til for eksempel ansatte i den aktuelle virksomheten.

5.1.3.3 Skytjenester

Det blir stadig vanligere at aktører i både privat og offentlig sektor tar i bruk skytjenester. Skytjenester er et samlebegrep for infrastruktur som gjerne leveres av tredjeparter, hvor lagring og prosesseringskapasitet spres utover forskjellige maskiner som i praksis kan være fysisk plassert hvor som helst. Bruken av skytjenester kan fremme sikkerhet og personvern ved at store tredjepartsleverandører kan ha bedre forutsetninger og midler for å iverksette sikkerhetstiltak, enn om alle virksomheter skal sørge for dette på egen hånd.

Samtidig kan bruken av skylagring skape utfordringer knyttet til både sikkerhet og personvern, dersom leverandørenes sikkerhetsrutiner svikter, for eksempel ved svak tilgangskontroll. Datamengden hos en skytjenesteleverandør vil som regel være langt større enn hos den enkelte behandlingsansvarlige, som kan gjøre slike tjenester til et attraktivt mål for kriminelle og andre uvedkommende. Det er også utfordringer knyttet til tilgangskontroll ved bruk av eksterne leverandører, dersom uautoriserte får adgang til informasjon som lagres i skyen.

Data som lagres «i skyen» er i praksis plassert på datamaskiner som ofte eies av en tredjepart, og

---

8 Personvernforordningen art. 32.

9 Zuboff, S. (2020). *Overvåkingskapitalismens tidsalder: Kampen for en menneskelig framtid ved maktens nye frontlinje*. Spartacus.

10 Ringnes, W. (2022). Kommersiell sporing – nasjonal risiko. *Internasjonal politikk 80*(1).

11 Wessel-Aas, J. (2017, 8. januar). *Digital grenseovervåkning utenfor lovlige grenser*. NRK Beta.

som kan være plassert i land med svakere personvernregulering enn vi har i Norge. Denne problemstillingen la grunnlaget for den såkalte Schrems II-dommen. I denne saken kom EU-domstolen til at Privacy Shield-avtalen var ugyldig som overføringsgrunnlag fordi den ikke ga et godt nok vern mot amerikanske etterretningsmyndigheters tilgang til personopplysninger om europeiske borgere (se boks 4.1). Konsekvensen av dommen er at aktører må ha et annet overføringsgrunnlag, noe som i praksis har gjort det svært vanskelig å overføre personopplysninger om individer som befinner seg i Europa, til USA.[12]

5.1.3.4 Tap av sikkerhet

Teknologiutviklingen kan beskrives som et våpenkappløp, hvor de som forsøker å styrke informasjonssikkerheten stadig utfordres av aktører som prøver å omgå informasjonssikkerhetstiltak. Et system som anses som sikkert i dag kan ende opp usikkert senere, enten på grunn av manglende oppfølging fra leverandøren, eller fordi ny teknologi gjør at dagens sikkerhetsstandarder blir utdaterte.

For eksempel har utviklingen av kvantedatamaskiner – svært kraftige maskiner som kan utføre ressurskrevende oppgaver – bidratt til at tidligere antatt sikre krypteringsløsninger kan knekkes. Det enorme tilfanget av offentlig tilgjengelige data, kombinert med tilgang til mer kraftfull analyseteknologi, har også bidratt til å gjøre det mer utfordrende å anonymisere data i dag enn det var tidligere. Studier har vist at man ved å sammenstille data fra flere kilder kan reidentifisere personer ved kun å kjenne til to datapunkter i et anonymisert datasett, som for eksempel postnummer og fødselsdato. Enkelte datatyper er mer utfordrende å anonymisere enn andre, for eksempel lokasjonsdata og genetiske.[13]

5.1.4 Personvernfremmende teknologi

Den teknologiske utviklingen innebærer ikke nødvendigvis bare en svekkelse av personvernet. I mange tilfeller vil utvikling og bruk av ny teknologi være viktige verktøy for å *styrke* og ivareta personvernet. *Personvernkommisjonen* vil ikke gjøre en omfattende gjennomgang av slike verktøy, men enkelte eksempler og trender beskrives kort nedenfor. En nærmere beskrivelse og drøfting av bruk av teknologiske verktøy for å ivareta og styrke rettigheter og plikter etter personopplysningsloven gjøres i kapittel 11.

5.1.4.1 Personvernvennlige utfordrere til teknologigigantene

Store deler av teknologimarkedet, særlig på forbrukersiden, domineres av et lite antall globale selskaper. Likevel har det vokst frem aktører som profilerer seg på personvernvennlige alternativer. Det inkluderer blant annet nettlesere som ikke sporer brukernes aktivitet, annonseplattformer som ikke bruker personopplysninger, samt søkemotorer som ikke analyserer brukerdata for å tilpasse søkeresultater. Som det skrives om i kapittel 9, er det en rekke konkurransemessige faktorer som bidrar til at få av disse aktørene har betydelige markedsandeler i dag.

5.1.4.2 Åpen kildekode

I motsetning til proprietær teknologi, som ofte er lukkede systemer beskyttet av opphavsrett og patenter, kan programvare bygget på *åpen kildekode* være et personvernvennlig alternativ. Åpen kildekode bidrar til at hvem som helst kan inspisere programvaren for å blant annet avdekke hva som foregår og hvilke data som samles inn. Det bidrar til en åpenhet som ofte ikke er tilgjengelig i proprietære systemer, hvor man som regel bare må stole på at tjenesteleverandører behandler personopplysninger på en ansvarlig måte.

5.1.4.3 Ende-til-ende-kryptering

Ende-til-ende-kryptering gjør kommunikasjon mellom enkeltindivider umulig å fange opp av tredjeparter ved at krypterte data kun kan leses av individer med tilgang på en unik krypteringsnøkkel. I ende-til-ende-kryptering er det kun individene som kommuniserer sammen som har tilgang på krypteringsnøklene, som i praksis betyr at selv ikke tjenesteleverandøren kan lese innholdet. For eksempel har krypterte meldingsapper blitt et viktig verktøy for demonstranter og for kommunikasjon mellom journalister og varslere.[14] På den andre siden kan ende-til-ende-kryptering i praksis gi kriminelle en trygg kanal for å utveksle ulovlig informasjon uten at politi og andre myndigheter kan fange det opp. Debatten rundt kryptering reiser grunnleggende spørsmål om forholdet mel-

[12] Stousland, C. & Førde, K. H. (2020, 19. oktober). *Privacy Shield kjent ugyldig: Hva nå?*. Digi.

[13] Datatilsynet. (2015). *Anonymisering av personopplysninger*.

[14] Schulz, W. & Hoboken, J. (2016). *Human rights and encryption*. UNESCO Publishing.

lom sikkerhet og personvern, og hvor samfunnet ønsker å trekke grensene mellom de to. Disse avveiningene drøftes videre i kapittel 7 om personvern i justissektoren.

5.1.4.4 Edge computing

Edge computing er en teknologi som tilrettelegger for behandling av data på lokale servere, som et motstykke til skytjenester som flytter behandlingen til eksterne servere.[15] Det skaper fordeler blant annet ved å redusere forsinkelser som kommer ved overføring av store mengder data, og kan også anvendes for å styrke informasjonssikkerhet og personvern ved å begrense dataflyt til eksterne aktører, som reduserer sårbarhetsflater. Det kan for eksempel skje ved å sette opp lukkede og krypterte nett innenfor begrensede fysiske områder, hvor behandling av personopplysninger skjer lokalt. Utviklingen av 5G-teknologi vil kunne gjøre det rimeligere å etablere slike nettverk, noe som kan styrke sikkerheten innen særlig utsatte områder, som for eksempel sykehus.

5.2 Særskilt utfordrende eksempler på teknologianvendelser med implikasjoner for personvernet

Som beskrevet ovenfor, har kombinasjonen av allestedsnærværende sensorer og sporingsteknologi, voksende lagrings-, overførings- og prosesseringskapasitet, samt kraftige maskinlæringssystemer, muliggjort databehandling i enorm skala. Nedenfor beskrives noen anvendelser av teknologi som er muliggjort av denne utviklingen, og som er særlig inngripende for personvernet.

5.2.1 Sporing og sammenstilling på tvers av plattformer og tjenester

Moderne sporingsteknologi gjør det mulig å samle inn personopplysninger gjennom nettsider, apper, betalingskort, tilkoblede produkter, og mye mer. Informasjonen kan sammenstilles og brukes til å skape svært omfattende profiler av enkeltindivider, eller for å segmentere individer i kategorier sammen med andre personer med lignende trekk. Det store plattformselskapene, som Alphabet, Meta og Amazon, er godt posisjonert til å sammenstille data på denne måten, da de har tilnærmet monopol på tjenestene de leverer og dermed mulighet til å samle inn opplysninger fra en enorm brukermasse.

Personopplysninger samles inn når vi aktivt deler informasjon om oss selv i for eksempel sosiale medier, men samles også inn passivt i bakgrunnen ved hjelp av sensorer og sporingsteknologier både når vi beveger oss rundt på nett og i det fysiske rom. Opplysningene blir gjerne sammenstilt og analysert ved hjelp av maskinlæringssystemer som kan utlede nye opplysninger om grupper eller individer basert på opplysningene. For eksempel kan opplysninger om bevegelsesmønster analyseres for å utlede hvor man bor og arbeider, om man har en religiøs tilhørighet, eller om man jevnlig sover borte hos andre. Opplysninger som i utgangspunktet ikke er veldig avslørende, kan dermed brukes til å utlede svært intime detaljer om den enkelte.

Når opplysninger samles inn på tvers av produkter og tjenester, blir det svært vanskelig for enkeltpersoner å ha oversikt over eller å forstå hvilke opplysninger som er samlet inn om dem, hvilke nye opplysninger som kan utledes fra opplysningene som er samlet inn, og hvilke anvendelsesområder og konsekvenser behandlingen av personopplysningene deres kan få, på kort og på lang sikt. Disse personvernutfordringene beskrives nærmere i kapittel 9 om forbrukeres personvern, men gjør seg også gjeldende dersom data sammenstilles og viderebehandles i for eksempel forvaltningen, justissektoren og arbeidslivssektoren.

Som beskrevet i kapittel 4 er dataminimering et grunnleggende personvernprinsipp – man skal ikke samle inn flere personopplysninger enn det som er nødvendig for behandlingsformålet. Dette prinsippet kan komme i konflikt med en grunnleggende forutsetning for mange maskinlæringssystemer, som er avhengig av å behandle mest mulig data uten at formålet med bruken nødvendigvis bestemmes i forkant.

5.2.2 Profilering og automatisert beslutningstaking

Den omfattende datainnsamlingen, sammenstillingen og analysen som er muliggjort av sporingsteknologi i kombinasjon med maskinlæring, har ført til at store mengder opplysninger kan anvendes til å lage omfattende profiler om enkeltindivider eller grupper.

Profilering defineres i personvernforordningen som «enhver form for automatisert behandling av personopplysninger som innebærer å bruke personopplysninger for å vurdere visse per-

[15] IBM. (u.å.) *What is edge computing?*

sonlige aspekter knyttet til en fysisk person, særlig for å analysere eller forutsi aspekter som gjelder nevnte fysiske persons arbeidsprestasjoner, økonomiske situasjon, helse, personlige preferanser, interesser, pålitelighet, atferd, plassering eller bevegelse».[16]

Slike profiler og segmenter kan brukes til å tilpasse tjenester til individer eller til grupper med særlige behov. Den kommersielle bruken av profilering til markedsføringsformål behandles i kapittel 9 om forbrukernes personvern. Offentlig forvaltnings bruk av profilering til kontrollformål behandles i kapittel 6 om den digitale offentlige forvaltningen.

5.2.2.1 Algoritmisk bias

Bruken av automatisk beslutningstaking på bakgrunn av profiler kan effektivisere prosesser innenfor en rekke samfunnsområder. Selv om dette i mange tilfeller vil være positivt, er det betydelige fallgruver dersom viktige beslutninger tas basert på slik teknologi.[17] Såkalt algoritmisk bias er et begrep som gjerne brukes for å beskrive skjevheter i datagrunnlag som brukes av et maskinlæringssystem, i selve modellen, eller i bruken av modellen. Algoritmisk bias kan blant annet oppstå dersom et maskinlæringssystem er trent opp på datasett som inkluderer feil, som ikke reflekterer virkeligheten, eller som reflekterer uønskede skjevheter som finnes i samfunnet.[18]

For eksempel har ansiktsgjenkjenningssystemer flere ganger vist seg å være dårligere på å korrekt identifisere individer med mørkere hudfarge,[19] og tekstanalyseteknologi har «lært» seg at kvinner er sykepleiere mens menn er doktorer.[20]

Bruken av avanserte maskinlæringssystemer kan føre til at samfunnsmessige urettmessigheter eller feilvurderinger blir legitimert og gitt et inntrykk av å være objektive sannheter, fordi beslutningene ble tatt av en datamaskin i stedet for et menneske. Dette kan ha svært alvorlige følger, for eksempel dersom et ansiktsgjenkjenningssystem brukt i forsøk på å bekjempe terrorisme identifiserer feil person som mistenkt, eller en selvkjørende bil ikke klarer å «se» enkelte grupper.

At slike problemer kan forekomme, betyr ikke at maskinlæring og kunstig intelligens ikke kan bidra til bedre beslutningstaking. Det betyr imidlertid blant annet at det må stilles strenge kontrollkrav til hvilke data som brukes og til hvilke formål man anvender teknologien.

5.2.2.2 Forklarbarhet og ansvar i automatiserte beslutningsprosesser

En av bekymringene i forbindelse med maskinlæring er at man ikke alltid vet hvordan resultatet blir produsert. Hvilke egenskaper, eller hvilke kombinasjoner av disse, var viktigst? Ofte vil modellen kun produsere et svar uten noen forklaring. Dersom slike systemer anvendes for å treffe beslutninger som påvirker mennesker i betydelig grad, og man ikke kan begrunne hvorfor beslutningen ble tatt, kan det være svært utfordrende for blant annet rettssikkerheten. Forklarbarhet og manuell vurdering av resultater er derfor særlig viktig i tilfeller hvor beslutninger basert på maskinlæring påvirker individer.

I situasjoner der maskinlæringssystemer brukes som et beslutningsgrunnlag, men et menneske tar den endelige beslutningen, kan det også oppstå problemer dersom mennesket ikke har forståelse eller kompetanse til å overprøve en anbefaling som eventuelt kan være feil. For eksempel, dersom et maskinlæringssystem som analyserer utvikling av kreft anbefaler et bestemt inngrep, og denne anbefalingen viser seg å være feil, kan det

Boks 5.3 Algoritmer, Data & Demokrati

Det danske prosjektet Algoritmer, Data & Demokrati har som mål å vurdere de demokratiske utfordringene ved at stadig flere beslutninger som har betydning for den enkeltes liv og samfunnets utvikling blir tatt på grunnlag av maskinlæringssystemer. Prosjektet skal blant annet munne ut i anbefalinger om tiltak for å sikre at demokratiske verdier ivaretas i utviklingen av algoritmer og databruk i offentlig sektor, samt generere innsikt og stimulere til offentlig debatt.[1]

[1] Algoritmer, Data & Demokrati. (u.å.). *ADD-projektet*.

[16] Personvernforordningen art. 4 nr. 4.

[17] European Commission. (2020). *White Paper On Artificial Intelligence: A European approach to excellence and trust*.

[18] PWC. (2022). *Understanding algorithmic bias and how to build trust in AI*.

[19] Burton-Harris, V. & Mayor, P. (2020, 24. juni). *Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart*. ACLU.

[20] Sun, T., Gaut, A., Tang, S., Huang, Y., ElSherief, M., Zhao, J., Mirza, D., Belding, E., Chang, K., Wang, W, Y. (2019). Mitigating Gender Bias in Natural Language Processing: Literature Review. *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*.

være vanskelig for helsepersonell å begrunne hvorfor de valgte å følge eller ikke følge anbefalingen. Utfordringer knyttet til å benytte maskinlæringssystemer til å fatte beslutninger som berører enkeltpersoner, er diskutert mer inngående i kapittel 6 om personvern i den digitale forvaltningen.

Ansvarsfordelingen er også utfordrende dersom et selvlærende produkt påfører skade. Dette har blitt satt på spissen i tilfeller hvor selvkjørende biler har kollidert, en utfordring som vil bli stadig mer aktuell når automatiserte prosesser tar over for menneskelig involvering.[21]

5.2.2.3 Tilsyn og kontroll med maskinlæringssystemer

I tråd med at stadig flere prosesser både i offentlig og privat sektor automatiseres og styres av maskinlæringssystemer, pågår det diskusjoner både nasjonalt og på europeisk nivå om hvordan en kan kontrollere at systemene ivaretar grunnleggende rettigheter og samfunnsprinsipper.

I forbindelse med forslaget til den kommende forordningen for kunstig intelligens, diskuteres det hvor ansvaret for å føre tilsyn med maskinlæringssystemer bør ligge.[22] Forordningsforslaget vil også stille krav om teknisk dokumentasjon og åpenhet knyttet til systemer som anses som høyrisiko, blant annet for å muliggjøre tilsyn og etterprøvbarhet av systemene. Forslaget til forordning for kunstig intelligens omtales nærmere i kapittel 9 om forbrukernes personvern.

I Norge har Riksrevisjonen satt i gang et samarbeid med riksrevisjoner i andre land for å undersøke mulige fremgangsmåter for å føre tilsyn med bruken av algoritmer i offentlig sektor.[23] Datatilsynet fører allerede tilsyn med maskinlæringssystemer som utfordrer personvernet,[24] og Finanstilsynet har en tilsvarende rolle ved bruk av slike systemer i finanssektoren.

5.2.3 Biometrisk analyse og fjernidentifikasjon

Biometri er en betegnelse for måling og registrering av data som er knyttet til et individs kropp, og inkluderer blant annet genmateriale, fingeravtrykk, ansikt, stemmeinformasjon, og ganglag. Biometrisk verifisering brukes gjerne til å bekrefte individers identitet, for eksempel som en del av sikkerhetsmekanismer, men kan også anvendes til overvåkningsformål.

I motsetning til enkelte former for personopplysninger, er det som regel umulig å endre biometriske data. For eksempel kan man ikke bytte fingeravtrykk dersom det kommer på avveie. Det er heller ikke mulig å skru av et fingeravtrykk eller et ansikt – man har det med seg overalt. Dersom man anvender teknologi for å identifisere individer basert på biometri, for eksempel ved at kamera på offentlige steder automatisk gjenkjenner individer basert på ansikt eller ganglag, er det derfor umulig for individer å velge å ikke bli registrert.

5.2.3.1 Audioanalyse

Audioanalyse kan blant annet brukes for å identifisere individer basert på stemmeleie og andre unike trekk i stemmen, noe som kalles stemmeavtrykk (voiceprinting). Lignende teknologi kan brukes til å registrere automatisk hva som blir sagt, for eksempel gjennom stemme-til-tekst-funksjoner.

Etter hvert som teknologien blir stadig kraftigere, kan den anvendes til å for eksempel plukke ut stemmer og samtaler fra bakgrunnsstøy. Slik bruk av audioanalyse muliggjør blant annet overvåkning av private samtaler uten at mennesker må aktivt avlytte et område eller en person. Utrullingen av slik teknologi vil legge nytt press på personvernet ved å tilrettelegge for automatisk avlytting, samt å kunne brukes til å opprette biometriske databaser til bruk i masseovervåkning.[25]

5.2.3.2 Biometrisk fjernidentifikasjon

Biometrisk fjernidentifikasjon («*remote biometric identification*») er en samlebetegnelse på bruken av biometri for å identifisere individer uten å ha fysisk tilgang på individets kropp. Det inkluderer automatisk registrering av blant annet ansikter, ganglag, stemmer og øyne, som fanges opp av

---

21 The Atlantic. (2018, 20. mars). *Can You Sue a Robocar?*.

22 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, Brussel, 21.april.2021 COM (2021) 206 final Artikkel 63

23 Riksrevisjonene i Finland, Nederland, Norge, Storbritannia og Tyskland. (2020). *Auditing machine learning algorithms: A white paper for public auditors.*

24 Datatilsynet. (2021, 16. juli). *Lukker IB-saken*.

25 Human Rights Watch. (2017, 22. oktober). *China: Voice Biometric Collection Threatens Privacy.*

sensorer og analyseres i sanntid uten at et menneske trenger å være involvert i prosessen.

Ansiktsgjenkjenning er et mye omtalt eksempel på biometrisk fjernidentifikasjon, og er allerede i bruk i flere samfunnssektorer. Teknologien brukes blant annet for å låse opp smarttelefoner eller dørlåser som en del av en sikkerhetsmekanisme.

Ansiktsgjenkjenning anvendes også i overvåkningsøyemed, for eksempel for å automatisk identifisere individer i videoopptak som ellers ville være svært arbeids- og ressurskrevende å gå gjennom manuelt.[26] Varianter av teknologien brukes også i forsøk på å gjenkjenne emosjonelle reaksjoner i ansiktsuttrykk. Det kan brukes til formål som å hjelpe funksjonsnedsatte med å identifisere ansiktsuttrykk, men er også attraktivt i markedsføringsøyemed. Det har også vært flere kontroversielle forsøk på å forsøke å utlede personlighetstrekk og andre egenskaper ut fra ansiktsanalyser.[27]

Det er store personvernutfordringer knyttet til bruken av biometrisk fjernidentifikasjon, særlig dersom teknologien brukes på offentlig sted. For eksempel er mulighetene for misbruk store dersom teknologien anvendes for å identifisere dissidenter eller demonstranter.[28]

På grunn av teknologiens svært inngripende natur, pågår det diskusjoner på europeisk nivå om hvorvidt bruk av ansiktsgjenkjenning i offentlige rom bør forbys.[29] I Norge har Teknologirådet foreslått at et forbud bør vurderes.[30] Datatilsynsmyndigheten for EU-organene (EDPS) har anbefalt et generelt forbud mot all biometrisk fjernidentifikasjon, på grunn av det de kaller en «ekstremt høy risiko for dype og udemokratiske inngrep i individers privatliv».[31] Som omtalt nærmere i kapittel 9 om forbrukernes personvern, vil den kommende EU-forordningen for kunstig intelligens innebære restriksjoner og et mulig forbud mot bruken av biometrisk fjernidentifikasjon i det offentlige rom.

Personvernkommisjonen støtter et generelt forbud mot bruk av biometrisk fjernidentifikasjon i offentlige rom. Norske myndigheter bør arbeide internasjonalt, særlig opp mot EU, for å få gjennomført et forbud.

5.2.3.3 *Datamanipulering og skillet mellom sant og usant*

I løpet av de siste årene har det pågått flere offentlige diskusjoner knyttet til bruken av kunstig intelligens for å manipulere lyd og video. Teknologien bak forfalskningene, som populært kalles «deepfakes», lar brukere mate et maskinlæringssystem med stemmedata eller bilder av ansikter, for å automatisk spleise det sammen med andre lydklipp eller videoklipp. Mye omtalte eksempler på bruk av teknologien inkluderer å manipulere lyd og bilder av politikere for å få det til å fremstå som at de sier noe de ikke har sagt i virkeligheten, samt misbruk knyttet til å manipulere pornografisk innhold.

Deepfake-teknologi er allerede tilgjengelig i programvare som kan brukes uten inngående teknisk kompetanse, som betyr at forfalskede lyd- og videoklipp kan florere.[32] Det har bidratt til bekymring om at man i fremtiden ikke vil kunne stole på egne øyne og ører, og at dette kan bidra til at faktiske video- og bildebevis kan avfeies med å hevde at det er snakk om deepfakes. På grunnlag av disse bekymringene, har enkelte tatt til orde for at teknologien bør forbys i sin helhet.[33]

Utviklingen og bruken av deepfake-teknologi forutsetter tilgang på store datamengder, og er særlig avhengig av å behandle videoer og bilder av ansikter. I mange tilfeller vil det være snakk om video av offentlige personer, fra offentlig tilgjengeliggjort materiale. Det skaper likevel personvernutfordringer når materiale som er lagret og tilgjengeliggjort for et bestemt formål behandles og brukes for helt andre formål. Det kan også være snakk om grove identitetskrenkelser dersom teknologien anvendes til å fremstille det som at et individ sier eller gjør noe de ikke har sagt eller gjort.

5.2.4 Nevro- og bioteknologi

Fremskritt innenfor nevro- og bioteknologi betyr at digitaliseringen også inntar kroppene og

---

[26] Teknologirådet. (2020). *Ansiktsgjenkjenning og personvern*.

[27] Venturebeat. (2021, 11. januar). *Outlandish Stanford facial recognition study claims there are links between facial features and political orientation*.

[28] Nature. (2020, 18. november). *The ethical questions that haunt facial-recognition research*.

[29] Politico. (2021, 6. oktober). *European Parliament calls for a ban on facial recognition.*

[30] Teknologirådet. (2020, 18. februar). *Når kunstig intelligens går på trynet. Dagens Næringsliv*.

[31] European Data Protection Supervisor. (2021, 23. april). *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary*.

[32] DW. (2022, 18. mars). *Fact check: The deepfakes in the disinformation war between Russia and Ukraine*.

[33] World Economic Forum. (2021, 1. april). *How to tell reality from a deepfake?*.

hodene våre. Det inkluderer blant annet implantater som kan opereres inn i kroppen, helseteknologiske verktøy for å måle kroppslige faktorer, individtilpasset medisin, samt implantater som kan registrere hjerneaktivitet.[34] Dette er et felt hvor oppsidene ved velfungerende teknologi er meget tydelige, da det kan bidra til betydelige helsefordeler, økt livskvalitet for sårbare grupper, og livreddende behandling. Samtidig er det ofte teknologi som behandler noen av de mest intime og sensitive opplysningene som finnes, og hvor risikoen ved sikkerhetsbrudd kan være svært høy. Dette gjør det særlig viktig at personvern og informasjonssikkerhet ivaretas i utviklingen av slik teknologi.

Genetiske data er et eksempel på særdeles sensitive personopplysninger som også kan ha stor nytteverdi, for eksempel i forskningsøyemed ved utvikling av medisiner. Dersom slike opplysninger kommer på avveie er det meget problematisk, da genetisk informasjon er unik for en person og kan gi opplysninger om egenskaper som i seg selv er sensitive, slik som sykdom og personlighetstrekk. Gener endrer seg ikke i løpet av livet, det er derfor en «livsløpsrisiko» dersom opplysningene kommer på avveie. Kommersiell bruk av genetiske data har blitt populært gjennom blant annet slektsforskningstjenester. Analyse av genetiske data for slike formål kan gi ny innsikt i slektskap, arvelige sykdommer og lignende, men reiser også en rekke etiske spørsmål knyttet til blant annet familiemedlemmers personvern, kommersiell gjenbruk og retten til å ikke vite.[35] Analyse av genetiske opplysninger kan ha uønskede effekter for andre enn individet som deler informasjonen, og kan misbrukes til diskriminerende formål dersom det ikke håndteres på en ansvarlig og etisk måte.

Nevroteknologi er teknologi som kan interagere direkte med nevroner i hjernen, og brukes blant annet innen forskning på sykdommer som Alzheimers. En rekke aktører forsøker å utvikle såkalte hjerne-datamaskin-grensesnitt (brain-computer-interfaces), med mål om å kunne registrere hjerneaktivitet eller styre teknologi med hjernen, enten gjennom utstyr som festes på hodet, eller som implantater som opereres inn i hodet. Etter hvert som teknologien blir mer avansert, kan dette føre til nye personvernutfordringer knyttet til individets tanker og underbevissthet. Bekymringer rundt dette har ført til at flere forskere på feltet har varslet om at det bør stadfestes rettigheter og prinsipper for å begrense personverninngripende teknologibruk på hjernen.[36]

5.3 Personvernkommisjonens syn på forholdet mellom teknologisk og samfunnsmessig utvikling

På samme måte som samfunnet kan påvirkes av teknologi, påvirkes den teknologiske utviklingen av samfunnets normer, regler og preferanser. I EU har man vedtatt at man ønsker en teknologisk utvikling fundamentert på europeiske verdier, og har utformet reguleringer for å styre utviklingen i ønsket retning.

Digitalisering er høyt på agendaen for norske politikere og myndigheter. Selv om digitalisering og teknologisk utvikling har bidratt til store gevinster i alle sektorer, er det viktig å understreke at digitalisering ikke er et mål i seg selv, men et middel for å øke velferd, effektivisere prosesser, og mye mer. Teknologi i seg selv kan brukes til gode og dårlige formål, og demokratisk kontroll må være et fundament for å sikre at samfunnet tar i bruk teknologi i fellesskapets interesse.

Personvernkommisjonen mener det er avgjørende at norske politikere har en grunnleggende teknologiforståelse, men uten at man blir fastlåst i en teknologideterministisk tilnærming, der grunnleggende prinsipper og rettigheter må vike for teknologien.

Personvernkommisjonen mener det bør være et grunnleggende samfunnsprinsipp at innføringen av inngripende teknologi ikke gjøres uten å ha kartlagt hvilke problemer man faktisk ønsker å løse, og at det gjøres grundige vurderinger av om det finnes mindre inngripende veier til målet.

Mangelfull ivaretakelse av personvernet kan være identitetskrenkende og skadelig for den enkelte, men som beskrevet i kapittel 3 har manglende personvern også en rekke andre negative følger som kan være særlig skadelig for samfunnet som helhet.

Personvernkommisjonen mener innføring og bruk av ny teknologi i samfunnet som kan medføre betydelige personvernkonsekvenser må være gjenstand for offentlig debatt. Det gjelder særlig hvis myndighetene ønsker å ta i bruk potensielt inngripende teknologi.

---

[34] Teknologirådet. (2020, 30. desember). *De viktigste teknologiske gjennombruddene i 2021*.

[35] Philips, A. M. (2016). Only a click away. DTC genetics for ancestry, health, love…and more: A view of the business and regulatory landscape. *Applied & Translational Genomics 8*.

[36] Politico. (2021, 31. august). *Machines can read your brain. There's little that can stop them*.

5.3.1 Føre-var-prinsippet

Den teknologiske utviklingen foregår i et raskt tempo. Hvilke konsekvenser innføringen av ny teknologi vil ha for den enkelte og for samfunnet, er i mange tilfeller omfattet av stor usikkerhet. Det er ofte først i ettertid at man ser hvilken effekt utviklingen har hatt på samfunnet. I mange tilfeller vil derfor normer, politikk og regelverk for anvendelse av teknologi komme i etterkant.

I utviklingen av regler og politikk for å beskytte miljø og klima står *føre-var-prinsippet* sentralt. Begrepet «the precautionary principle» ble utviklet innenfor the World Charter for Nature, som ble vedtatt av FNs generalsekretær i 1982. Prinsippet er deretter implementert i ulike internasjonale konvensjoner som tar sikte på å beskytte miljøet. Føre-var-prinsippet har etter hvert også fått stor gjennomslagskraft utover rene miljøspørsmål. I hovedsak innebærer prinsippet at der hvor det foreligger trussel om alvorlig eller uopprettelig skade, skal ikke mangel på fullstendig vitenskapelig visshet kunne brukes som begrunnelse for å utsette kostnadseffektive tiltak for å hindre skade. *Usikkerhet* om skadevirkninger skal altså ikke bety at man unnlater å iverksette tiltak.[37]

Grunntanken bak føre-var-prinsippet kan overføres til ivaretagelsen av personvernet. Etter *Personvernkommisjonens* syn bør ikke usikkerhet knyttet til hvorvidt innføringen av en teknologisk løsning vil ha alvorlige konsekvenser for ivaretakelsen av personvernet, brukes som grunn til å avstå fra å sette inn beskyttelsestiltak. Usikkerheten bør tvert imot *være en grunn* til å iverksette forebyggende tiltak.

Personvernkommisjonen mener at før teknologi med særlig høy risiko for personvernet vurderes innført, som for eksempel biometrisk fjernidentifikasjon i offentlige rom, bør føre-var-prinsippet komme til anvendelse.

5.4 Personvernkommisjonens anbefalinger oppsummert

- *Personvernkommisjonen* støtter et generelt forbud mot bruk av biometrisk fjernidentifikasjon i offentlige rom. Norske myndigheter bør arbeide internasjonalt, særlig opp mot EU, for å få gjennomført et forbud.
- *Personvernkommisjonen* mener det er avgjørende at norske politikere har en grunnleggende teknologiforståelse, men uten at man blir fastlåst i en teknologideterministisk tilnærming, der grunnleggende prinsipper og rettigheter må vike i teknologiens tjeneste.
- *Personvernkommisjonen* mener det bør være et grunnleggende samfunnsprinsipp at innføringen av inngripende teknologi ikke gjøres uten å ha kartlagt hvilke problemer man faktisk ønsker å løse, og at det gjøres grundige vurderinger av om det finnes mindre inngripende veier til målet.
- *Personvernkommisjonen* mener innføring og bruk av ny teknologi i samfunnet som kan medføre betydelige personvernkonsekvenser må være gjenstand for offentlig debatt. Det gjelder særlig hvis myndighetene ønsker å ta i bruk potensielt inngripende teknologi.
- *Personvernkommisjonen* mener at før teknologi med særlig høy risiko for personvernet vurderes innført, som for eksempel biometrisk fjernidentifikasjon i offentlige rom, bør føre-var-prinsippet komme til anvendelse.

[37] NOU 2000: 29 *GMO-mat – Helsemessige konsekvenser ved bruk av genmodifiserte næringsmidler og næringsmiddelingredienser.* Kap. 6.

Del II
Personvernets situasjon og utfordringer innen utvalgte sektorer

Kapittel 6
Personvern i den digitale forvaltningen

6.1 Innledning

Personvernkommisjonen skal ifølge mandatet kartlegge «offentlig sektors behandling av personopplysninger til andre formål enn innsamlingsformålet, og gi en vurdering av de negative personvernkonsekvensene ved dette sett opp mot fordelene». *Kommisjonen* tolker oppdraget til å innebære en drøftelse av den pågående digitalisering av offentlig forvaltning, og den økte bruken og delingen av personopplysninger dette innebærer. *Kommisjonen* legger særlig vekt på problemstillinger knyttet til deling og viderebehandling av personopplysninger, profilering og bruk av kunstig intelligens i forvaltningen.[1]

Bruk av personopplysninger i offentlig forvaltning handler dypest sett om spørsmålet om hvilke verdier vi vil verne om og hvordan maktbalansen mellom offentlige myndigheter og den enkelte borger er ivaretatt. Den norske velferdsstaten er et velfungerende system og offentlig forvaltning nyter høy tillit i befolkningen. Det handler om hvordan offentlig forvaltning må organiseres slik at velferdsmodellen fungerer i tråd med samfunnets verdier og forventninger.

Digitalisering kan bidra til en effektiv, brukerorientert og rettssikker offentlig forvaltning, og realiserer viktige samfunnsgevinster. Digitalisering kan fjerne unødige arbeidsprosesser og kan dermed frigjøre ressurser til annet viktig arbeid. Informasjonsinnhentingen kan være mer effektiv, analysene bedre og saksbehandling kan bli raskere og bedre opplyst. God bruk av digitale verktøy kan bidra til økt tillit og transparens, likebehandling og rettssikkerhet. Å utnytte potensialet som ligger i digitalisering innebærer imidlertid ofte økt deling og viderebehandling av personopplysninger.

Offentlig forvaltning behandler store mengder personopplysninger om alle innbyggerne, fra de er født inntil de dør. Dette innebærer en betydelig infrastruktur av data om innbyggerne, ofte med fødselsnummer som identifikator. Behandling av personopplysninger gir det offentlige kunnskap om befolkingen, som er en forutsetning for at velferdsstaten kan fungere. Samtidig vil digitalisering av offentlig forvaltning kunne åpne for at personopplysninger som samles inn brukes til nye formål. For eksempel vil forvaltningen kunne bruke personopplysninger for å klassifisere, predikere eller kontrollere innbyggernes atferd. Dette kan ha negative konsekvenser for personvernet.

Det er derfor viktig at digitalisering i offentlig forvaltning skjer på en måte som sikrer den enkelte innbyggers autonomi og integritet, samt at den høye tilliten i befolkningen ivaretas. De mulighetene digitaliseringen gir, må vurderes opp mot våre ønsker for hvordan offentlig forvaltning og velferdsstaten skal utvikle seg fremover. Dette innebærer å finne den riktige balansen mellom personvern og effektive, brukervennlige og rettferdige tjenester i offentlig forvaltning.

Målet for digitaliseringspolitikken er å «tilrettelegge for en åpen og samordnet forvaltning som har høy tillit i befolkningen», som skal ivareta innbyggernes «rettssikkerhet, bidra til at beslutninger er faglig basert, ivareta demokratiske verdier og fremme effektiv bruk av ressursene».[2]

I dette kapitlet vurderer *Personvernkommisjonen* fordeler og utfordringer knyttet til bruk av personopplysninger som følger av økt digitalisering i offentlig forvaltning. *Personvernkommisjonen* vil foreslå tiltak regjeringen bør iverksette for å ivareta innbyggernes personvern og rettssikkerhet, og ivareta tilliten til offentlig forvaltning.

6.1.1 Hovedtrekk i digitaliseringspolitikken

Digitaliseringspolitikken for offentlig forvaltning kommer til uttrykk i stortingsmeldinger, strategier, planer og ulike typer veiledere som formidler

[1] Personvernkommisjonen benytter begrepet viderebehandling, som også er benyttet i personvernforordningen, for å omtale bruk av personopplysninger til et annet formål enn det opprinnelige innsamlingsformålet. Viderebehandling kan være forenlig eller uforenlig med innsamlingsformålet, jf. personvernforordningen art. 6 nr. 4.

[2] Prop. 1 S (2021–2022) *For budsjettåret 2022 under Kommunal- og distriktsdepartementet.*

prinsipper og metoder for digitaliseringsarbeidet i offentlig forvaltning. Eksempler er «Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet»,[3] «Digitaliseringsstrategi for offentlig sektor, 2019–2025»,[4] «Nasjonal strategi for kunstig intelligens»,[5] og stortingsmelding «Data som Ressurs».[6]

Den norske digitaliseringspolitikken påvirkes i stor grad av strategier og regulering fra EU. En av Europakommisjonens seks hovedprioriteringer for 2019–2024 er digitalisering. I strategien «A Europe Fit for a Digital Age» foreslås flere regelverksinitiativer som vil påvirke og sette rammer også for digitaliseringen av offentlig forvaltning i Norge.[7] Hovedtrekk i både norsk og europeisk digitaliseringspolitikk er å øke digitaliseringstakten for å forbedre tjenestene for innbyggerne.

Norsk offentlig forvaltning skal oppleves sammenhengende og helhetlige av brukerne, uavhengig av hvilke offentlige virksomheter som tilbyr dem. Med brukerne menes både innbyggere, frivillig sektor og offentlige og private virksomheter.

Den gjeldende digitaliseringsstrategien oppfordrer derfor blant annet til deling av personopplysninger på tvers av forvaltningsorganer for å realisere «kun-én-gang»-prinsippet. Innbyggere skal kun måtte gi fra seg sine opplysninger én gang til forvaltningen i stedet for å måtte avlevere opplysninger flere ganger til ulike forvaltningsorganer.

«Kun én gang»-prinsippet er også fastsatt i Digitaliseringsrundskrivet avsnitt 1.2, hvor det fremgår at utvekslingen skal skje på en måte som bevarer dataenes autentisitet og integritet.[8] Utveksling av data som andre offentlige virksomheter har krav på, skal prioriteres.

En måte å realisere «kun én gang»-prinsippet på er å benytte «fellesløsninger» fremfor at hvert forvaltningsorgan etablerer sin egen, og sørge for at fellesløsninger virker på tvers av forvaltningsnivåer og sektorer. Fellesløsningene er åpne og gjenbrukbare løsninger som har felles grensesnitt og datagrunnlag. Løsningene inkluderer blant annet flere fellesregistre som folkeregisteret, samt felles grensesnitt for dialog med myndigheter (Altinn), innlogging og autentisering (ID-porten). Noen registre er tilgjengelig for bruk av flere forvaltningsorganer, for eksempel folkeregistret, kontakt- og reservasjonsregistret og matrikkelen.[9] Offentlige virksomheter kan hente ut relevante opplysninger fra disse registrene i stedet for å aktivt måtte innhente dem fra innbyggerne.

«Kun én gang»-prinsippet legger blant annet grunnlaget for utvikling av «sammenhengende tjenester» på tvers av virksomheter og sektorer. Arbeidet med sammenhengende tjenester er i stor grad knyttet til prioriterte livshendelser som det å få barn, å starte en bedrift eller dødsfall og arv. Her samarbeider flere offentlige virksomheter på tvers for å sømløst tilby ulike tjenester som er relevante for innbyggere i den aktuelle livshendelsen.

Digitaliseringspolitikken skaper en forventning om viderebehandling av personopplysninger enten ved deling av opplysninger mellom forvaltningsorganer eller økt bruk av fellesregistrene. Et av tiltakene i Digitaliseringsstrategien for offentlig sektor (2019–2025) var å etablere et nasjonalt res-

Boks 6.1 «Oppgjør etter dødsfall»

Et eksempel på en sammenhengende tjeneste er prosjektet «Oppgjør etter dødsfall/Altinn dødsbo». I dag oppleves prosessen for oppgjør av bo etter dødsfall tungvint og tidkrevende for de etterlatte. Den er manuell og papirbasert, byråkratisk og mange parter er involvert.

Formålet med prosjektet er å forenkle prosessen etter dødsfall gjennom digitalisering og deling av data i prosesser som i dag er kompliserte og papirbaserte. Det er et samarbeidsprosjekt mellom Digitaliseringsdirektoratet, Brønnøysundregistrene, domstolene, finansnæringen, Skatteetaten, Statens kartverk og Statens vegvesen.[1]

[1] Bits. (u.å.) *Oppgjør etter dødsfall*.

[3] Prop. 1 S (2021–2022) *For budsjettåret 2022 under Kommunal- og distriktsdepartementet*.

[4] Kommunal- og distriktsdepartementet. (2019). *Én digital offentlig sektor: Digitaliseringsstrategi for offentlig sektor 2019-2025*. Merk at denne strategien er felles for statlig og kommunal forvaltning.

[5] Kommunal- og distriktsdepartementet. (2020). *Nasjonal strategi for kunstig intelligens*.

[6] Meld. St. 22 (2020–2021) *Data som ressurs – Datadrevet økonomi og innovasjon*. Kommunal- og distriktsdepartementet.

[7] European Commission. (2022). *A Europe fit for the digital age*. Noen initiativer kommer i form av forordninger som vil legge føringer for hvordan offentlig sektor kan dele og bruke personopplysninger. Dette er for eksempel Digital Governance Act, og i enkelte tilfeller, Forordning for kunstig intelligens.

[8] Rundskriv H-5/21 *Digitaliseringsrundskrivet*, Kommunal- og distriktsdepartementet.

[9] Kommunal- og distriktsdepartementet. (2021). *Hva er fellesløsninger?*.

surssenter for deling av data som en del av Digitaliseringsdirektoratet.

Ressurssenteret ble åpnet i 2020 og tilbyr rådgivning og veiledning knyttet til deling av data. Videre skal senteret være læringsmiljø og kompetansebank for hele offentlig sektor og ha spisskompetanse på sammenhengen mellom juss, teknologi og forretnings- og forvaltningsprosesser.[10] Begrunnelsen for etablering av senteret var at vurderingene ved deling og bruk av data kan være svært krevende. Dette skyldes blant annet at vurderingene berører flere regelverk som må sees i sammenheng, herunder personvernregelverket, og innebærer vekting av flere hensyn.

Digitaliseringsstrategien fastslår at personvern og informasjonssikkerhet er «grunnleggende i digitaliseringsarbeidet og må være et innebygd element fra starten av».[11] Det understrekes også at digitaliseringen skal ivareta innbyggernes rettssikkerhet og personvern, og sikre at offentlig sektor fortsatt har høy tillit. Digitaliseringsstrategien sier imidlertid lite om *hvordan* dette skal gjøres. Etter *Personvernkommisjonens* vurdering har personvernhensyn fått for liten plass i digitaliseringen av offentlig sektor. I dette kapitlet vil *Personvernkommisjonen* komme med vurderinger og forlag til tiltak for å bedre den helhetlige ivaretakelsen av personvern i digitaliseringsarbeidet fremover.

6.1.2 Viktigheten av tillit til offentlig forvaltning

Digitalisering i offentlig sektor innebærer ofte økt bruk av personopplysninger. Bruken begrenses blant annet av regler om taushetsplikt, behandlingsgrunnlag, formålsbegrensning, krav til datakvalitet, regler om likestilling og diskriminering og andre forvaltningsrettslige regler. Reglene er satt for å verne om innbyggernes integritet og autonomi, og bidrar til å sikre innbyggernes tillit til offentlig forvaltning.

I motsetning til bruk av personopplysninger i privat sektor, der behandlingen av personopplysninger gjerne baseres på samtykke fra den «registrerte», avtale eller legitim interesse, baserer offentlig sektors behandling seg typisk på lov eller forskrift. Den registrerte kan derfor i svært begrenset grad påvirke om eller hvordan forvaltningen skal behandle personopplysningene. I tillegg oppstiller personvernregelverket en rekke unntak[12] fra de registrertes rettigheter i behandlingsgrunnlagene som er mest relevante for offentlig forvaltning.[13] Forholdet mellom den registrerte og myndighetene, bærer preg av en asymmetrisk maktbalanse. Det påhviler derfor offentlig forvaltning en særlig forpliktelse til å opptre på en måte som er egnet til å skape og bevare innbyggernes tillit.

Tillit til offentlige myndigheter er en forutsetning for et velfungerende demokrati. Høy tillit, både i befolkningen generelt og til myndighetene, gir myndighetene bedre forutsetninger for å kunne håndtere kriser som covid-19-pandemien eller økonomiske nedgangstider på en god måte. I 2021 målte OECD norske borgeres tillit til myndighetene til 77 %. Dette er blant de høyeste tillitsnivåene og langt over snittet i OECD-landene på 47 %.[14]

Åpenhet og informasjon er viktig for befolkningens tillit til offentlig forvaltning.[15] Forvaltningsorganers holdninger til og rutiner for å behandle innbyggernes personopplysninger er med på å påvirke tilliten. Manglende tillit kan føre til at innbyggere avstår fra å bruke offentlige tjenester, som for eksempel kan føre til at man går glipp av informasjon og risikerer å ikke kunne hevde sine rettigheter.

Uten tillit vil digitaliseringspolitikken, med mål om å blant annet gi bedre tjenester, økt rettssikkerhet og effektivitet, vanskeligere la seg gjennomføre.

Også den årlige innbyggerundersøkelsen viser at offentlig sektor i Norge er velfungerende og nyter høy tillit blant innbyggerne.[16] Ifølge undersøkelsen fra 2021 har befolkningen ganske høy tillit til myndighetenes behandling av personopplysninger. Innbyggerne har derimot lav tillit til myndighetenes evne til å ivareta informasjonssikkerheten. Økt bevissthet om personvern, blant annet etter hendelser som dataangrep mot Stortinget[17] og Østre Toten kommune[18] som har fått

---

10 Kommunal- og distriktsdepartementet. (2019). *Én digital offentlig sektor: Digitaliseringsstrategi for offentlig sektor 2019-2025*.

11 Kommunal- og distriktsdepartementet. (2019). *Én digital offentlig sektor: Digitaliseringsstrategi for offentlig sektor 2019-2025*.

12 Se personvernforordningen art. 14 nr. 5 bokstav c, art. 17 nr. 3 bokstav b og art. 20 nr. 3.

13 Se personvernforordningen art. 6 bokstavene c og e.

14 OECD. (2022). *Drivers of Trust in Public Institutions in Norway*.

15 Utenriksdepartementet/Delegasjonen til OECD og UNESCO (2021, 1. mars). *Et nytt paradigme for tillit til myndighetene*.

16 Direktoratet for forvaltning og økonomistyring (DFØ). (2021). *Innbyggerundersøkelsen 2021*. Innbyggerundersøkelsen er en måling av omdømmet i befolkningen til ulike offentlige tjenester som gjennomføres med to års mellomrom. Undersøkelsen gir et kunnskapsgrunnlag til departementer, direktorater, kommuner og fylkeskommuner i deres planleggings- og prioriteringsarbeid.

Boks 6.2 Tillit til offentlige institusjoner

I Datatilsynets personvernundersøkelse 2019/2020 kommer det fram at helse- og skattevesenet og politiet har størst tillit i befolkningen når det kommer til ivaretagelse av personvern, med over 80 % tillitsgrad.[1] Rundt 60 % har tillit til kommunenes, etterretningstjenestens og NAVs behandling av personopplysninger. Tillit til behandlingen av personopplysninger i skolen og barnehagen er noe lavere. Med enkelte unntak, har respondentene større tillit til offentlige enn private virksomheter.

55 % av respondentene i Datatilsynets undersøkelse opplyser at de har avstått fra å benytte en tjeneste på grunn av usikkerhet knyttet til hvordan personopplysninger blir behandlet. Spørsmålet skiller ikke mellom private eller offentlige tjenestetilbydere.

[1] Datatilsynet. (2020). *Personvernundersøkelsen 2019/2020*.

mye oppmerksomhet i media, kan ha bidratt til lavere tillit.

Digitalisering av offentlig forvaltning muliggjør i større grad viderebehandling av personopplysninger på tvers av virksomheter og tjenester. For at tilliten til forvaltningen skal ivaretas hos brukerne er det viktig at viderebehandlingen av personopplysningene skjer i tråd med innbyggernes forventninger. Som beskrevet i kapittel 3, kan personvern sees i kontekstuelt perspektiv. Det kan oppleves som et tillitsbrudd om opplysninger som er samlet inn for et konkret formål brukes til nye formål i en annen kontekst.

6.2 Hvordan bruker offentlig forvaltning personopplysninger i en digital hverdag?

6.2.1 Hvordan digitaliseres den offentlige forvaltningen?

I likhet med samfunnet ellers, har offentlig forvaltning vært gjenstand for en omfattende digitalisering. Dette er ikke noe nytt, digitalisering i samfunnet og offentlig forvaltning har pågått siden 60-tallet.[19] Hastigheten har imidlertid økt i takt med tiden. Med dagens digitalisering står offentlig forvaltning overfor en rekke muligheter og utfordringer.

Digitaliseringen av offentlig forvaltning omfatter mange ulike elementer og handler om mer enn automatisering av vedtak. Deler av digitaliseringen er innføringen av ulike digitale verktøy og hjelpemidler for å forbedre arbeidet i forvaltningen, slik som løsninger for tekstbehandling og samhandlingsverktøy. Viktige deler av digital forvaltning gjelder automatisering av rettsanvendelsen. Dette kan skje ved at datamaskiner automatiserer deler av saksbehandlingen og gir støtte til saksbehandler (jf. «beslutningsstøttesystemer»). Men det kan også skje ved at systemet er programmert til å fatte vedtak uten at en saksbehandler er involvert i den enkelte sak, og det er resultatet fra maskinen som utgjør vedtaket, uten kontroll fra et menneske (jf. «beslutningssystemer»).[20] I alle deler av forvaltningens bruk av digitale løsninger kan det behandles personopplysninger.

Gode digitale løsninger kan bidra til å sikre personvernet. Velutviklede løsninger kan gi god personopplysningssikkerhet og gi god kontroll på flyten og bruken av personopplysninger. Dette bidrar til å ivareta prinsippene for behandling av personopplysninger, slik som dataminimering, riktighet, lagringsbegrensning, og integritet og konfidensialitet. Videre kan gode digitale løsninger gi et godt grunnlag for å utvikle automatiserte tjenester som gjør det lettere for den registrerte å ivareta sine rettigheter etter personvernforordningens kapittel 3.

Motsetningsvis vil dårlige digitale løsninger kunne svekke personvernet. Tekniske løsninger kan ha utilstrekkelig informasjonssikkerhet eller være utformet slik at de oppfattes som lite transparente. Dette kan svekke tilliten til offentlig forvaltning.

Selv om digitaliseringen av offentlig forvaltning kan omfatte mye, fokuseres det i det videre på automatiseringen av rettsanvendelse, profilering og bruk av maskinlæring i forvaltningen.

[17] Stortinget. (2021, 19. mars). *Stortinget utsatt for IT-angrep*.

[18] Datainnbruddet hos Østre Toten kommune beskrives i avsnitt 6.4.7.

[19] Stensrud, T.I. (2020). *Retten i det digitale Norge. Senter for rettsinformatikk, 1970-2020*. Bergen Fagbokforlaget. s. 94-95.

[20] Husbanken benyttet seg av helautomatiserte systemer i behandlingen av bostøtte allerede i 1972. Stensrud, T.I. (2020). *Retten i det digitale Norge. Senter for rettsinformatikk, 1970-2020*. Bergen Fagbokforlaget.

6.2.2 Automatisert rettsanvendelse

Automatisert rettsanvendelse innebærer at en datamaskin bruker rettsreglene automatisk i stedet for at en saksbehandler bruker rettsreglene manuelt. Men for at dette skal være mulig, må forvaltningen på forhånd ha fortolket alle lover, forskrifter og andre rettskilder og uttrykt tolkningsresultatene som algoritmer i en programkode. Datamaskinen er altså forhåndsprogrammert med de rettsregler forvaltningen mener skal gjelde, slik at reglene kan anvendes på konkrete saker.

For å automatisere rettsanvendelse er det særlig to slags systemer som er aktuelle:[21]

Rettslige beslutningssystemer. Dette er systemer som helt eller delvis automatiserer behandling av enkeltsakene fram til vedtak. Et beslutningssystem kan gjerne forutsette noe manuell saksbehandling, men det er resultatet systemet kommer frem til som legges til grunn for vedtak. Det er altså ingen person som ved ordinær saksbehandling overprøver det systemet har kommet frem til.

Rettslige beslutningsstøttesystemer. Dersom det er mennesker som i hovedsak behandler sakene og har kontroll over og kan overprøve resultatene fra datamaskinsystemene, kalles systemene beslutningsstøttesystemer. Også slike systemer kan ha deler der rettsanvendelsen er automatisert, men det er uansett saksbehandler som innestår for resultatene (vedtakene).

Automatisering av vedtak består av automatisk innhenting av informasjon (typisk, personopplysninger), og videre bruk av disse opplysningene for å prøve om lovens vilkår er oppfylt og for å foreta kompliserte beregninger, for eksempel av studiepoeng, skatter og sosiale stønader. For at dette skal kunne skje, er rettsreglene «oversatt» til kjørbar programkode, dvs. til detaljerte og uttømmende beskrivelser (algoritmer) som angir hva maskinen må gjøre for å komme frem til vedtak som er i samsvar med loven. Når sakene gjelder enkeltpersoner, er det personopplysninger som er input til systemet. Selve vedtaket (output) er nye personopplysninger om den saken gjelder. I personvernperspektiv kan vi si at personopplysninger blir brukt som «råstoff» for å produsere nye personopplysninger.

Personvernregelverket gjør et viktig skille mellom systemer som behandler personopplysninger på helt automatiserte måter, og andre systemer der det skjer noe manuell behandling. Er behandlingen helt automatisert har registrerte personer rett til å be om «relevant informasjon om den underliggende logikken» for behandlingen av personopplysninger. Beslutningsstøttesystemer er aldri helt automatiserte. Rettslige beslutningssystemer *kan* være helt automatiserte, men ofte er det noe manuell saksbehandling som gjør at systemet likevel ikke blir omfattet av de spesielle reglene for helt automatiserte systemer.

Det er svært utbredt i norsk forvaltning å bruke beslutningssystemer og beslutningsstøttesystemer for å treffe vedtak i saker om enkeltpersoner. Automatiseringsgraden er ofte høy, og det er en politisk målsetting at den skal øke. For eksempel brukes slike høyt automatiserte systemer av Skatteetaten for å fatte skattevedtak; av Lånekassen for vedtak om lån og stipend; av Folketrygden for å vedta alderspensjon; og av Husbanken for å avgjøre krav om bostøtte.

Automatisert rettsanvendelse kan bidra til å ivareta viktige hensyn i forvaltningen:

- Automatisert rettsanvendelse kan gjøre det lettere å sikre hensynet til likebehandling. En datamaskin som får to helt like saker, vil alltid komme til det samme resultatet. Korrekt automatisert rettsanvendelse kan dermed forhindre urettmessig og utilsiktet forskjellbehandling.
- Automatisert rettsanvendelse *kan* gi god gjennomsiktighet og forutberegnelighet. Det vil alltid være mulig å følge algoritmen for å forstå den nøyaktige årsaken til resultatet av automatisert saksbehandling. De fleste mennesker kan imidlertid ikke lese programkode. Gjennomsiktige systemløsninger er derfor først og fremst en mulighet, og krever at forvaltningen har dokumentert hvilke regler som er programmert inn i systemet. Med slik dokumentasjon kan folk lese forklaringer i vanlig språk og slipper å prøve å forstå programkoden.
- Automatisert rettsanvendelse kan gi stor forutberegnelighet. Dersom det er kjent hvilke opplysninger datamaskinen skal behandle og hvordan behandlingen skjer, vil det være mulig å undersøke hva som blir resultatet av et vedtak før det er fattet. Det kan for eksempel utvikles løsninger hvor innbyggerne kan gå inn på nettsiden til en offentlig etat og eksperimentere med hvilke vilkår som må være oppfylt for at et bestemt vedtak skal fattes. Dette gjør at innbyggerne kan se hva de selv må endre på eller oppdatere.[22]

---

[21] Digitaliseringsdirektoratet. (u.å). *Hel eller delvis automatisering?*. og Schartum, D.W. (2018). *Digitalisering av offentlig forvaltning – Fra lovtekst til programkode*. Fagbokforlaget. s. 22.

– Automatisering av rettsanvendelse kan bidra til å ivareta hensynet til effektivitet, både for forvaltningen og for innbygger. Det vil være en fordel for innbyggerne å få effektive tjenester. Vedtak kan fattes raskt slik at innbyggerne enkelt kan få avklart sin rettigheter og plikter. Ressursene som spares når tjenester automatiseres kan brukes på andre viktige oppgaver.

Automatisert rettsanvendelse har også ulemper, blant annet:
– Effektivitetsgevinsten ved automatisert rettsanvendelse skyldes at en datamaskin kan behandle vedtak raskt og i store mengder. Dette betyr samtidig at feil i systemet vil kunne gi feil i mange vedtak. Datamaskinen følger dataprogrammet slavisk, enten det er riktig eller feil.
– Når forvaltningen fastsetter hvilke rettsregler som skal programmeres inn i systemet, står de overfor små og store tolkningsvalg. Det kan derfor forekomme at andre tolkningsvalg enn de som ligger i programkoden er rettslig akseptable. Det kan være vanskelig å oppdage muligheten for å velge andre fortolkninger enn de forvaltningen har lagt til grunn i systemet. Derfor er det viktig at forvaltningen dokumenterer det rettslige innholdet i systemene sine.
– Automatisert rettsanvendelse forutsetter ferdigtolkede rettsregler som deretter brytes ned til instruksjoner som kan gjøres til et dataprogram.[23] Blant annet fastsettes det på uttømmende måte hvilke personopplysninger som er relevante i saken, og hvordan disse kan inngis i systemet. Dermed kan det skje at konkrete saksforhold ikke blir tatt hensyn til selv om personen saken gjelder mener de er relevante.
– Forvaltningsskjønn kan ikke automatiseres.[24] For eksempel kan man ikke automatisere beslutninger om hva som er «rimelig». En kan heller ikke automatisere når et forvaltningsorgan «kan» treffe en avgjørelse. Poenget med forvaltningsskjønn er at det skal skje konkrete vurderinger, og da er det ikke mulig å forhåndsprogrammere dem. I mange sammenhenger ønsker personene vedtaket gjelder nettopp en mulighet for konkret skjønnsmessig, individuell vurdering i deres sak. Med helt automatiserte vedtak er ikke det mulig, og derfor kan slike vedtak oppfattes som «firkantete» og urettferdige av personer som representerer spesielle tilfeller.

6.2.3 Maskinlæring

Maskinlæring er en spesialisering innenfor kunstig intelligens, og innebærer bruk av «statistiske metoder for å la datamaskiner finne mønstre i store datamengder».[25] Dette er nærmere beskrevet i kapittel 5. I offentlig forvaltning er det mange problemstillinger hvor det kan være aktuelt å benytte maskinlæring som en del av løsningen. Dette kan være problemstillinger som omfatter bruk av personopplysninger.

Maskinlæring kan ikke brukes til å automatisere rettsanvendelse slik det er beskrevet i avsnitt 6.2.2. Grunnen er at rettsanvendelse handler om å følge regler i lov og forskrift, ikke om statistiske beregninger. Maskinlæring kan imidlertid brukes som beslutningsstøtte for å bruke forvaltningsskjønn i tidligere saker til å ta stilling til skjønn i nye, lignende saker. Hvis en finner tidligere saker som ligner en foreliggende sak, kan det for eksempel være sannsynlig at sakene bør få samme utfall. Den konkrete skjønnsmessige vurderingen må likevel en saksbehandler gjøre, der tidligere saker maskinlæringssystemet har funnet frem til, inngår i grunnlaget for vedtaket.

Bruk av maskinlæringssystemer i offentlig forvaltning kan gi mange muligheter, men kan også medføre personvernutfordringer. Blant mulighetene er avanserte former for profilering.[26] Slik kan for eksempel velferdsordninger tilbys til innbyggere med spesielle behov uten at vedkommende er nødt til å selv oppsøke hjelp, eller helsekontroller kan tilbys til befolkningsgrupper som antas å være i risikosoner basert på en rekke opplysninger.[27]

Selv om maskinlæringssystemer kan brukes til mange gode formål, er det egenskaper ved maskinlæring som det er grunn til å være opp-

[22] Se f.eks. Skatteetaten. Skattekalkulator. En oversikt over slike systemer finnes i Slotten, S. & Schartum, D.W. (2021). Selvbetjent rettshjelp. *CompLex 3/2021*.

[23] Digitaliseringsdirektoratet. (u.å). *Datamaskiners muligheter og begrensninger ved automatisert rettsanvendelse*.

[24] Digitaliseringsdirektoratet. (u.å). *Skjønn gjør automatisering vanskelig*.

[25] Tidemann, A. & Elster, A. C. (2022). *Maskinlæring*. Store norske leksikon

[26] Som beskrevet i kapittel 5, kan kraftige statistiske analyseverktøy brukes til å analysere store mengder data for å finne nye mønstre og sammenhenger. Dette kan anvendes i forsøk på å forutse sannsynligheten for at visse hendelser vil inntreffe. For eksempel kan et slikt system kalkulere risiko for at en person vil ha vanskeligheter med å betjene et lån, eller at en befolkningsgruppe er særlig utsatt for enkelte sykdommer.

[27] Teknologirådet. (2017). *Denne gangen er det personlig*.

merksom på (personvernutfordringer knyttet til bruk av maskinlæringssystemer er også beskrevet i kapittel 5). Egenskaper ved maskinlæring som det er grunn til å ta særlig hensyn til ved bruk i offentlig sektor er:

- *Datamengde:* Flere maskinlæringsalgoritmer er avhengig av store mengder data. Dette kan støte an mot dataminimeringsprinsippet. Utvikling og bruk av maskinlæring krever også ofte mange *forskjellige* typer personopplysninger – opplysninger som ofte er samlet inn for andre formål. Dette kan støte an mot formålsbegrensningsprinsippet. Ivaretakelse av prinsippene om dataminimering og formålsbegrensning er helt grunnleggende for at enkeltindividet skal ha kontroll over personopplysningene sine.
- *Datakvalitet:* Det kan være mangler eller feil i dataene som analyseres, eller i dataene som systemet trenes på. Samtidig kan det gjøres feil ved utvalg av data som skal analyseres eller brukes som treningsdata. Dette kan føre til at feil gjenskapes og forsterkes, slik at det introduseres systematiske skjevheter (bias) i systemet som kan føre til diskriminerende effekter. På den måten kan det oppstå fare for at vi trekker med oss holdninger i et historisk datamateriale som vi i dag tar avstand fra.
- *Transparens:* Avanserte former for maskinlæring kan være vanskelig både å forstå og forklare, og kan gjøre det tilnærmet umulig å forklare hvordan opplysninger blir koblet og vektlagt i en spesifikk behandling. De matematiske og statistiske modellene maskinlæring er basert på, gjør det videre vanskelig å forstå og kontrollere om det er systematiske feil eller skjevheter i datasettet (bias), og hvordan dette virker inn på resultatene. Dersom maskinlæringssystemene er uforståelige «svarte bokser» uten åpenhet og mulighet til å forklare og motsi resultatene fra systemet, kan dette underminere viktige prinsipper om demokrati og rettssikkerhet.
- *Ukritisk bruk av resultatene fra statistiske analyser (beslutningsstøttesystemer):* Maskinlæring er basert på statistiske analyser og resultatene kan derfor aldri legges direkte til grunn som vedtak. Maskinlæring kan derfor bare brukes som beslutnings*støtte*. Når vedtak fattes, foreligger det risiko for at myndighetene likevel ukritisk legger til grunn resultatene som systemet genererer. Årsaken kan for eksempel være lange restanser, stort arbeidspress og urealistisk tiltro til systemet eller manglende kunnskap om hva et maskinlæringssystem er. I avsnitt 6.2.5 omtales et eksempel fra Nederland hvor myndighetene ukritisk la til grunn resultatet fra et beslutningsstøttesystem. Dette er ikke et problem ved teknologien selv, men ved hvordan den brukes.

En rapport skrevet på oppdrag for Europaparlamentet trekker frem de samme risikofaktorene som nevnt over ved bruk av maskinlæring i offentlig sektor.[28] I rapporten foreslås det en rekke tiltak for å motvirke disse fallgruvene. Tiltakene inkluderer blant annet obligatoriske menneskerettighetsvurderinger, etablering av regulatoriske sandkasser og kompetansebygging.

Det er i dag flere regelverk som innebærer krav til offentlig forvaltnings bruk av maskinlæringssystemer som behandler personopplysninger. Blant disse er Grunnloven, EMK, personopplysningsloven, likestilling- og diskrimineringsloven og forvaltningsloven. Dette er imidlertid generelle regelverk som har betydning for maskinlæring uten å regulere slik teknologi spesielt. På EU-nivå ser en imidlertid behovet for direkte og mer presis regulering av kunstig intelligens, herunder maskinlæring. I forslaget til forordning for kunstig intelligens forslår Europakommisjonen en risikobasert tilnærming, og hoveddelen av lovforslaget gjelder systemer der det er høy risiko. I forslaget settes det også en grense for hva som er uakseptabel høy risiko, og teknologi som faller innenfor denne kategorien forbys. Et eksempel på teknologi som er på forbudslisten i forslaget er systemer for «social credit scoring», som gir innbyggere poengsummer basert på oppførsel. Slike systemer er utviklet og er i bruk i Kina, og Europakommisjonen ønsker å forby innføring av lignende systemer i Europa. Maskinlæringssystemer der det *ikke* er høy risiko er ikke omfattet av forslaget til EU-regler. Mange mulige anvendelser av maskinlæring i offentlig forvaltning med relativt lav risiko er derfor ikke omfattet av forslaget. Også for enkelte slike anvendelser kan det være behov for lovregulering.

6.2.4 Forholdet mellom maskinlæring og profilering

Med «profilering» sikter man til kategorisering av personer basert på likhetstrekk og korrelasjoner i et datagrunnlag, og eventuelt til å foreta avgjørelser basert på tilhørighet til en gruppe eller kate-

[28] Policy Department for Economic, Scientific and Quality of Life Policies. (2021). *ArtificiaI Intelligence and public service.*

gori. Profilering er definert i personvernforordningen artikkel 4 nr. 4 som:

> «enhver form for automatisert behandling av personopplysninger som innebærer å bruke personopplysninger for å vurdere visse personlige aspekter knyttet til en fysisk person, særlig for å analysere eller forutsi aspekter som gjelder nevnte fysiske persons arbeidsprestasjoner, økonomiske situasjon, helse, personlige preferanser, interesser, pålitelighet, atferd, plassering eller bevegelser.»

Profilering vil typisk innebære at eksisterende personopplysninger brukes til å vurdere sannsynligheten for at den registrerte tilhører en viss type kategori, har bestemte egenskaper eller sannsynligheten for en viss type handling/atferd i fremtiden. Fordi det er spørsmål om sannsynlighet, vil ikke profileringen gi eksakte svar. Svarene og kvaliteten på disse beror på hvilke personopplysninger som benyttes og bruken av disse, herunder hvilket spørsmål som søkes besvart.

Korrelasjoner tilsvarer ikke nødvendigvis kausalitet.[29] Dette betyr at profileringen kan avdekke sammenhenger, uten at det er årsaks-sammenheng. Videre kan profileringen gi sammenhenger som vi i vår rettsstat ikke ønsker, eller tillater, at skal være en del av en vurdering. [30]

Profilering i vid forstand trenger ikke nødvendigvis å inkludere maskinlæring. Maskinlæring er imidlertid godt egnet til å lage profiler. Maskinlæring brukes blant annet til å vurdere sannsynligheten for en bestemt atferd, såkalt prediktiv analyse, som nevnt over. Ved prediktiv analyse beregner maskinlæringsalgoritmen, på basis av personopplysninger fra en stor gruppe mennesker, seg frem til en persons sannsynlige fremtidige handlinger og egenskaper. Når slutninger om en enkeltperson foretas basert på egenskaper til en gruppe mennesker fremfor en reell individuell vurdering, oppstår det såkalte *«gruppe-til-individ-problem»*. Det gir en risiko for feil, vilkårlighet, urettferdighet og diskriminering i avgjørelsene. Dette er bakgrunnen for at personvernforordningen har et forbud mot helautomatiserte avgjørelser basert på profilering i artikkel 22, ved siden av regler som krever åpenhet, informasjon og innsyn i hvordan personopplysninger behandles.

[29] Dahlum, S. & Grønmo, S. (2021). *Kausalitet*. Store norske leksikon.

[30] Eksempelvis likestilling- og diskrimineringslovgivning, forvaltningsrettens lære om hensyn som ikke kan tillegges vekt i ved skjønnsutøvelse og personvernforordningens artikkel 5 nr. 1 bokstav a om rettferdighet.

6.2.5 Eksempler på bruk av maskinlæring i norsk og utenlandsk offentlig forvaltning

Bruk av maskinlæring, herunder profileringsmodeller, kan brukes både til gunst og til ugunst for enkeltindividet. På den ene siden kan forvaltningen profilere en person for å vurdere om det er behov for ekstra oppfølgning og støtte. Profilering kan også brukes for å påvirke atferd, for eksempel gjennom tilpasset veiledning. Avhengig av omstendighetene kan dette anses for å være til gunst for den som profileres. Videre kan profilering tenkes brukt til kontroll av forvaltningen til gunst for enkeltindividet, for å påse at det ikke er fattet uriktige vedtak mot visse typer individer. På den andre siden kan profilering også benyttes til ugunst for enkeltindividet som profileres. Forvaltningen kan eksempelvis ønske å profilere innbyggere for å vurdere om noen er risikoobjekter som bør tas ut for nærmere kontroll. Profilering, uavhengig av om den er til gunst eller ugunst for enkeltindividet, reiser en rekke personvernspørsmål. Profilering for kontrollformål reiser i tillegg rettssikkerhetsspørsmål slik som spørsmål om legalitetsprinsippet og uskyldspresumpsjonen. *Personvernkommisjonen* adresserer de særlige utfordringene knyttet profilering for kontrollformål i avsnitt 6.4.5.

I internasjonal sammenheng har profilering ved hjelp av maskinlæring særlig vært brukt til kontrollformål og innenfor barnevern. I Danmark har myndighetene testet ut et slik system, den såkalte «Gladsaxe-modellen». Formålet med modellen var å sile bekymringsmeldinger til barnevernet for å vurdere nærmere oppfølging, og for å fange opp utsatte barn på et tidlig stadium. Ved bruk av maskinlæring til kontrollformål er det gjerne snakk om å identifisere risikofaktorer for juks og andre avvik ved mottakelse av ytelser. I Norge benytter Skatteetaten slike systemer for å sørge for en mer målrettet kontroll og for å differensiere oppfølgingen av skatteytere.[31] Nav benytter ulike systemer for beslutningsstøtte, men det er uklart om det benyttes profilering til kontroll. I Navs tildelingsbrev for 2022 er det uttrykt at Nav skal jobbe med å utarbeide risikoanalyser for å identifisere områder som er særlig utsatt for trygdesvindel.[32]

Personvernkommisjonen ønsker under å løfte frem eksempler på bruk av maskinlæring i offent-

[31] Finansdepartementet. (2018). *Høyring – forslag om endringar i reglane om informasjonshandsaminga i Skatteetaten*.

lig forvaltning, med særlig fokus på profilering, som kan reise personvernutfordringer.[33]

Nav

Nav har deltatt i Datatilsynets sandkasse for kunstig intelligens, hvor etaten ønsket å bruke maskinlæring til å forutse hvilke sykemeldte brukere som lå an til å bli langtidssykmeldte. Ved å benytte en maskinlæringsmodell som profilerte den sykmeldte var målet å gi automatisert beslutningsstøtte til den Nav-ansatte. Den Nav-ansatte skulle ved hjelp av resultatet fra profileringen videre vurdere hvilken oppfølging fra Nav-kontoret den sykmeldte hadde behov for. Prosjektet ble lagt på is da det var usikkerhet knyttet til lovhjemler for utviklingen av algoritmen, da dette forutsatte behandling av store mengder personopplysninger om et betydelig antall personer som ikke lenger er sykemeldte.

Danmark

I desember 2021 vedtok det danske Folketinget endringer i skattekontrolloven som gir Skatteforvaltningen hjemmel til å sammenstille alle sine data og til å innsamle all nødvendig informasjon til kontrollformål. Formålet er å utvikle og benytte algoritmer for å understøtte regjeringens ønske om å styrke Skatteforvaltningens muligheter for å utføre en bedre og mer intelligent kontroll.

Lovendringen består av to deler.[34] Den ene er en hjemmel for å samkjøre opplysninger Skatteforvaltningen er i besittelse av for å utvikle blant annet maskinlæringsmodeller og analytiske modeller. Den andre er en hjemmel for å innsamle ytterligere informasjon som deretter kan sammenstilles med informasjon Skatteforvaltningen allerede har. Dette kan være informasjon fra offentlig tilgjengelige kilder, for eksempel fra eBay, Amazon og Google Maps.

Opplysningene skal videre kunne sammenstilles for å finne frem til nye opplysninger om den enkelte. Forskriftshjemmelen er også ment å gi hjemmel til å fravike formålsbestemthetsprinsippet i personvernforordningen.

Når det gjelder muligheten for at risikomodellene kan peke ut feil kontrollobjekter, er vurderingene som er gjort knyttet til dette, begrenset til tilfeller hvor algoritmene ikke klarer å identifisere *alle* risikoobjekter. Risikoen for at en modell *feilaktig* utpeker personer eller virksomheter som mulige skattesvikere er ikke nevnt.

Lovendringene ble enstemmig vedtatt i Folketinget. Det var først etter at loven var vedtatt at det ble offentlig debatt.[35] I etterkant har flere representanter i Folketinget hevdet at de ikke forsto rekkevidden av lovforslaget de vedtok eller at de hadde betenkeligheter, men ikke så noe alternativ.

Nederland

I perioden 2012–2019 benyttet den nederlandske skattemyndigheten et maskinlæringssystem for å flagge personer som hadde høy antatt risiko for å misbruke landets barnetrygdordning. Maskinlæringssystemet ble ikke brukt til å fatte enkeltvedtak, men som beslutningsstøtte.

I ettertid ble det avdekket at mellom 25 000 og 35 000 hadde blitt feilaktig anklaget for trygdemisbruk på bakgrunn av systemet. Anklagene førte til krav om tilbakebetaling av ytelser, med svært alvorlige konsekvenser for innbyggerne som ble rammet. Systemet opererte med en stor mengde variabler, inkludert opplysninger om statsborgerskap. Det var mange feil i systemet, blant annet at innbyggere med dobbelt eller ikke-nederlandsk statsborgerskap ble flagget som mulige misbrukere i mye større grad enn innbyggere med nederlandsk statsborgerskap. Individets nasjonalitet ble et utvelgelseskriterium for kontroll, selv om dette ikke var et faktisk vilkår for å få støtte. Bruken av det automatiserte systemet førte således til ulovlig diskriminering med både psykologiske og økonomiske skadevirkninger for de som ble rammet.

Eksemplet fra Nederland illustrerer noen av problemstillingene som kan oppstå ved bruk av maskinlæringssystemer som beslutningsstøtte. Utviklingen av maskinlæringssystemet og bruken av data var utilstrekkelig. Saken var svært alvorlig, men det er grunn til å understreke at det ikke bare var maskinlæringssystemet som var utfordringen.

---

32 Lintvedt, M. N. (2022). *Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering*. Utredning for Personvernkommisjonen. Jf. Arbeids- og velferdsdirektoratet. (2022). *Tildelingsbrev til Arbeids- og velferdsdirektoratet for 2022*. Punkt 3.3.2.

33 Den grunnleggende teknologiske utviklingen som ligger bak disse anvendelsene beskrives nærmere i kapittel 5. Flere av eksemplene er hentet fra rapporten *Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering*, skrevet av Mona Naomi Lintvedt på oppdrag fra *Personvernkommisjonen*.

34 Se Lovforslag nr. L 73 Folketinget 2021–2022 *Forslag til Lov om ændring af lov om et indkomstregister, skatteindberetningsloven og skattekontrolloven*.

35 Busse, J. (2022, 10. januar). *Ny lov giver Skat indsigt i, hvor meget du satte din kaffemaskine til salg for på Den Blå Avis*. Alltinget.

Det var en svært omfattende systemsvikt hvor flere lag med rettsikkerhetsmekanismer feilet.

Et av elementene i systemsvikten var den menneskelige kontrollen. Systemet var et beslutningsstøttesystem. Det skulle snevre inn gruppen som skulle vurderes for kontroll, men ikke selv ta den endelige avgjørelsen. En saksbehandler skulle gjøre dette. Saksbehandleren hadde imidlertid begrenset innsikt i hvorfor en person var flagget og la derfor ukritisk til grunn at alle som ble flagget av systemet antageligvis hadde misbrukt ordningen.[36]

I januar 2021 gikk den nederlandske regjeringen av som en følge av skandalen. I tillegg til barnetrygdskandalen, har Nederland vært rystet av to andre saker med visse likhetstrekk.[37] Sakene viser hvordan kompleksitet og manglende transparens gjør samspillet mellom mennesker og maskin utfordrende.

Eksemplene over viser at det kan være utfordringer ved å bruke maskinlæring i forvaltningen. Det er viktig å se til andre og ta lærdom av de erfaringene som er gjort. Ved bruk av maskinlæring vil det være ekstra viktig å legge inn egnede tiltak for å sikre de registrertes rettigheter, sørge for egnede garantier mot feilbruk og å verne om sårbare grupper. Særlig er dette av stor betydning der bruk av maskinlæring inngår i behandling som er av inngripende karakter, for eksempel til kontroll. Teknologien må testes grundig før den tas i bruk og jevnlig revideres mens behandlingen pågår.

6.3 Rettslige rammer for behandling av personopplysninger i offentlig forvaltning

Digitalisering i offentlig forvaltning innebærer ofte behandling av personopplysninger. Personvernregelverket gir rammene for hvordan personopplysninger kan behandles, men må sees i sammenheng med annen lovgivning og rettsprinsipper. Offentlig forvaltnings behandling av personopplysninger vil kunne anses som et inngrep i personvernet, og må da skje innenfor de rammene som følger av Grunnlovens § 113, EMK artikkel 8 og Grunnloven § 102.

I det følgende beskrives de rettslige rammene for behandling av personopplysninger i offentlig forvaltning. Det gis først et generelt overblikk over krav til behandlingsgrunnlag før det ses nærmere på hvordan kravet til lovregulering av behandlingsformål påvirker bruk og deling av personopplysninger i offentlig forvaltning.

6.3.1 Legalitetsprinsippet og krav om rettsgrunnlag etter Grunnloven og EMK

I norsk rettstradisjon står legalitetsprinsippet helt sentralt. Legalitetsprinsippet innebærer at staten ikke kan gjøre inngrep i borgernes rettsstilling uten hjemmel i lov. Prinsippet er grunnlovfestet i Grunnloven § 113 som lyder: «myndigheters inngrep ovenfor den enkelte må ha grunnlag i lov».

Grunnloven § 102 lyder:

> «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.
>
> Statens myndigheter skal sikre et vern om den personlige integritet.»

Denne bestemmelsen skal leses som at systematisk innhenting, oppbevaring og bruk av opplysninger om andres personlige forhold bare kan finne sted i henhold til lov, benyttes i henhold til lov eller informert samtykke og slettes når formålet ikke lenger er til stede.[38]

Bestemmelsen gir ikke adgang til eller vilkår for å gjøre inngrep i rettigheten, men har en klar sammenheng med Grunnloven § 113. Høyesterett har lagt til grunn at inngrep i rettighetene i § 102 kan skje dersom tiltaket har en tilstrekkelig hjemmel, forfølger et legitimt formål og er forholdsmessig.[39]

Grunnloven har klare likhetstrekk med EMK artikkel 8, og må tolkes i lys av denne.[40] Den Europeiske Menneskerettighetsdomstolen (EMD) har i sin praksis lagt til grunn at offentlige myndigheters lagring av personopplysninger som

---

36 Lintvedt, M. N. (2022). *Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering*. Utredning for Personvernkommisjonen.

37 System Risico Indicatie (SyRI) som brukte en algoritme for å målrette kontroll ved å vurdere risiko for om personer ville jukse med trygd eller skatt. Case of NJCM c.s./De Staat der Neder–landen (SyRI) before the District Court of The Hague (case number: C/09/550982/HA ZA 18/338). Fraud Signa–ling Facility (FSV) Og Fraud Signaling Facility (FSV) som lagret opplysninger om skattytere og som ble bruk til å flagge potensielle skattesvikere hos skatteetaten i Nederland: Autoriteit Persoongegevens. (2021). *Tax Administration fined for discriminatory and unlawful data processing*.

38 Inst. 186 S (2013–2014). *Innstilling til Stortinget fra kontroll- og konstitusjonskomiteen*, punkt 2.1.9. s. 27

39 Rt. 2014 side 1105 avsnitt 28 og Rt. 2015 side 93 avsnitt 60.

40 Rt. 2015 side 93 avsnitt 57.

knytter seg til privatliv, utgjør et inngrep i retten til privatliv. Et slikt inngrep må oppfylle kravene i EMK artikkel 8 nr. 2, som krever at inngrepet må ha tilstrekkelig hjemmel, ha et legitimt formål og være forholdsmessig. Det er kravet om tilstrekkelig hjemmel som er særlig interessant i denne sammenhengen.

Hjemmelskravet innebærer at behandling av personopplysninger av offentlig forvaltning må ha et rettsgrunnlag. Det stilles ikke formelle krav, som gjør at rettsgrunnlaget kan være lov, forskrift eller uskreven rett.[41] Det stilles imidlertid krav om at rettsgrunnlaget skal være tilgjengelig og forutberegnelig.

Hva som er et tilstrekkelig rettsgrunnlag for offentlig sektors behandling av personopplysninger, beror på en konkret vurdering, blant annet av hvor inngripende behandlingen er. Desto større inngrepet er, desto strengere krav til klarhet og forutberegnelighet. Dette betyr at et større inngrep vil ha strengere krav til presisjonsgrad i hjemmelsgrunnlaget. I noen tilfeller må hjemmelsgrunnlaget detaljere ikke bare hvorfor behandlingen finner sted, men også hvordan.

6.3.2 Krav til behandlingsgrunnlag etter personopplysningsloven

Det følger av personvernforordningen at all behandling av personopplysninger må ha et behandlingsgrunnlag for å være lovlig. Dette er beskrevet i denne utredningens kapittel 4. Reglene om behandlingsgrunnlag følger av personvernforordningen artikkel 6, og for noen typer opplysninger artikkel 9 og 10. For behandling av personopplysninger i offentlig forvaltning vil særlig grunnlagene i artikkel 6 nr. 1 bokstav c og e være aktuelle.[42] Disse behandlingsgrunnlagene er relevante når behandling av personopplysninger er *nødvendig for å*

- oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige.
- «utføre en oppgave i allmennhetens interesse» som den behandlingsansvarlige er pålagt; eller
- «utøve offentlig myndighet» som den behandlingsansvarlige er pålagt. [43]

Det følger av artikkel 6 nr. 3 at «grunnlaget for behandlingen» nevnt i nr. 1 bokstav c og e skal «fastsettes» i unionsretten eller i nasjonal rett. Dette innebærer at artikkel 6 nr. 1 bokstav c eller e ikke alene kan utgjøre behandlingsgrunnlaget, men at det må finnes et *supplerende* rettsgrunnlag for behandlingen i nasjonal rett.

Når det gjelder spørsmål om *hva* som kan utgjøre det supplerende rettsgrunnlag, legger departementet i forarbeidene til grunn at lov- og forskriftsbestemmelser kan utgjøre supplerende rettsgrunnlag og antar at også vedtak fattet i medhold av lov eller forskrift omfattes.[44]

Når det gjelder spørsmål om innholdet i rettsgrunnlaget, utdyper fortalepunkt 45 nærmere hvor detaljert det rettslige grunnlaget i nasjonal rett må være. Her kommer det frem at for behandlinger som utføres i samsvar med en rettslig forpliktelse som påhviler den behandlingsansvarlige, for eksempel et offentlig forvaltningsorgan (artikkel 6. nr. 1. bokstav c – rettslig forpliktelse) skal det supplerende rettsgrunnlag være tydelig på at behandling av personopplysninger er nødvendig for å innfri den rettslige forpliktelsen. Den rettslige forpliktelsen må altså være tydelig fastsatt, men ikke uttrykkelig den behandlingen av opplysninger som dette innebærer.

For behandling av personopplysninger som er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet, (artikkel 6. nr. 1 bokstav e) er det tilstrekkelig at det supplerende rettsgrunnlaget gir grunnlag for å utøve myndighet eller å utføre en oppgave i allmennhetens interesse. Det er altså ikke nødvendig at det supplerende rettsgrunnlaget uttrykkelig regulerer behandling av personopplysninger.

Det fremkommer videre av artikkel 6 nr. 3 at det rettslige grunnlaget *kan* inneholde særlige bestemmelser om (blant annet) de generelle vilkårene som skal gjelde for lovligheten av behandlingen, hvilke type opplysninger som skal behandles og hvilke enheter personopplysninger kan utleveres til.

Det foreligger dermed et absolutt krav om at myndighetsutøvelsen, eller oppgaveløsning i den allmenne interesse, skal fremkomme av rettsgrunnlaget. I tillegg må formålet med behandlingen fremgå når det gjelder behandlinger som er nødvendig for å oppfylle en «rettslig forpliktelse».

---

41 S. and Marper v. The United Kingdom [GC], no.30562/04 and no. 30566/04, (2008), ECHR 1581

42 Art. 6 nr. 1 bokstav f «berettiget interesse» kan i noen tilfeller være relevant for offentlig forvaltning, men ikke dersom behandlingen er en del av 'myndighetsutøvelse'.

43 Private vil også kunne ha rettslige forpliktelser til å behandle personopplysninger, og private vil kunne utføre oppgaver i allmennhetens interesse. Drøftelsen nedenfor er imidlertid avgrenset til offentlig forvaltning, dvs. forutsetningen er at den behandlingsansvarlige som har/bruker de nevnte rettslige grunnlagene er et forvaltningsorgan.

44 Prop. 56 LS (2017–2018) *Lov om behandling av personopplysninger (personopplysningsloven)*

Derimot foreligger det ikke noe absolutt krav om at det i lov eller forskrift må detaljeres hvilke personopplysninger som skal inngå i behandlingen. Det kreves heller ikke en særlig lovbestemmelse for hver enkelt behandling, hvilket betyr at flere ulike behandlinger kan utføres i medhold av samme rettslige grunnlag.

Når det ovenfor er sagt at det ikke er nødvendig å fastsette detaljerte regler i lov og forskrift, betyr det samtidig at det er *anledning* til å gjøre nettopp det. Forordningen tillater for eksempel at det gis nasjonale bestemmelser om hvilken type opplysninger som skal behandles, om hvem personopplysningene kan utleveres til, om formålene for behandlingen, og hvor lenge opplysningene kan lagres.

6.3.3 Samlet om krav til lovregulering av behandlingsformål

Kort oppsummert betyr dette at personvernforordningens krav om supplerende rettsgrunnlag utfylles av de menneskerettslige kravene til rettsgrunnlag for inngrep i retten til privatliv. Kravene om supplerende rettsgrunnlag må derfor også ses i lys av rettspraksis fra blant annet EMD.[45]

Personvernforordningen krever, i noen tilfeller, at det finnes et supplerende rettslig grunnlag, mens legalitetsprinsippet og EMK i tillegg stiller ytterlige krav til det rettslige grunnlaget.

Dette innebærer at for behandling av personopplysninger i offentlig forvaltning, må det foretas en vurdering av formålet med behandlingen, samt en vurdering av hvor inngripende behandlingen er.

En slik vurdering kan, etter omstendighetene, innebære at det supplerende rettsgrunnlaget må inneholde mer spesifikke bestemmelser enn det som uttrykkelig fremgår av minimumskravene etter personvernforordningen artikkel 6 nr. 2 og 3.

6.3.4 Rettslige rammer for viderebehandling av personopplysninger i offentlig forvaltning

Utgangspunktet, basert på redegjørelsen over, er at det supplerende rettsgrunnlag må kunne svare på *hvorfor* det er nødvendig at personopplysninger blir behandlet. Det er ikke krav til, men rettslig adgang til å fastsette *hvordan* opplysningene kan behandles.

For behandling av personopplysninger i offentlig forvalting vil formålsangivelsen typisk gjelde utøvelse av ulike typer myndighet, for eksempel til å treffe bestemte typer enkeltvedtak. Formål kan også være knyttet til andre forvaltningsoppgaver, som for eksempel kvalitetsforbedring, informasjonsarbeid, eller intern administrasjon.

Personvernprinsippene, og særlig prinsippet om formålsbegrensning, setter imidlertid grenser for hva personopplysninger kan brukes til etter at de er samlet inn. Artikkel 5 nr. 1 bokstav b fastsetter at personopplysninger skal samles inn for «spesifikke, uttrykkelig angitte og berettigede formål og ikke videre behandles på en måte som er uforenlig med disse formålene.»

Formålsangivelsen er i første omgang relevant for vurdering av om et offentlig forvaltningsorgan har behandlingsgrunnlag for å samle inn og behandle opplysninger til de oppgavene forvaltningsorganet er pålagt på lovgivningstidspunket.

Det kan oppstå spørsmål om forvaltningsorganer har anledning til å bruke allerede innsamlede personopplysninger til andre formål som ikke var forutsett på det tidspunktet da myndighetsutøvelsen for vedkommende organ ble lovfestet.

I mandatet er *Personvernkommisjonen* bedt om å se nærmere på offentlig sektors behandling av personopplysninger til *andre formål enn innsamlingsformålet*. *Personvernkommisjonen* har valgt å forstå formuleringen «andre formål» i mandatet som henvisning til *videre formål*. For sekundære formål[46] gjelder det særlige krav, men disse vil ikke bli drøftet i det følgende.

6.3.5 Vurdering av forenlighet

For å kunne bruke allerede innsamlede personopplysninger til videre formål, altså andre formål enn det opplysningene opprinnelig ble samlet inn for, må det vurderes om de nye formålene er *forenlige* med innsamlingsformålene.

Dersom det nye formålet med behandlingen er forenlig, vil behandling være tillatt uten et eget separat rettsgrunnlag for viderebehandlingen. Dersom det nye formålet ikke er forenlig med innsamlingsformålet, må viderebehandlingen ha grunnlag i lov eller samtykke. Om det trengs et nytt grunnlag i lov for selve viderebehandlingen er derfor avhengig av en forenlighetsvurdering.

---

[45] Se også personvernforordningens fortalepunkt 41.

[46] Sekundære formål brukes som fellesbetegnelse på typer formål som direkte er angitt i forordningen, og som en uansett kan behandle personopplysninger til, selv om de ikke er angitt som innsamlingsformål eller videre formål. Dette gjelder «arkivformål i allmenhetens interesse», «formål knyttet til vitenskapelig eller historisk forskning», og «statistiske formål».

Denne forenlighetsvurderingen må skje i samsvar med personvernforordningen artikkel 6 nr. 4. Det skal blant annet tas hensyn til enhver forbindelse mellom formålene som personopplysningene er blitt samlet inn for, og formålene med den tiltenkte viderebehandlingen, i hvilken sammenheng personopplysningene er blitt samlet inn, særlig med hensyn til forholdet mellom den registrerte og den behandlingsansvarlige, personopplysningenes art, især om det er særlige kategorier av personopplysninger, de mulige konsekvensene av den tiltenkte viderebehandlingen for de registrerte, og om det foreligger nødvendige garantier (for eksempel kryptering eller pseudonymisering).

Det kan være vanskelig å gjøre en forenlighetsvurdering når det gjelder videre behandling av personopplysninger i offentlig forvaltning. For offentlig forvaltnings behandling av personopplysninger basert på personvernforordningen artikkel 6 nr.1 bokstav e, er det som nevnt ikke nødvendig at selve formålet for *behandlingen* fremgår av rettsgrunnlaget. Selv om formålet ikke trenger å fremgå av rettsgrunnlaget, er det ikke gitt unntak fra formålsbegrensningsprinsippet.

Det er ikke anledning for lovgiver til å lovfeste enhver type uforenlig videre bruk i nasjonal rett. Slike lovbestemmelser må være et «nødvendig og forholdsmessig tiltak i et demokratisk samfunn for å sikre oppnåelse av målene nevnt i artikkel 23 nr. 1».[47]

Personvernkommisjonen mener det er viktig å avklare hva slags videre bruk av personopplysninger i offentlig forvaltning som vil være akseptabel, samt hvem som kan/bør foreta disse vurderingene. Det er uklart om det er nok at hvert enkelt forvaltningsorgan som behandlingsansvarlig gjør disse vurderingene, eller om de bør gjøres av lovgiver.[48]

6.3.6 Andre rettslige skranker for bruk av opplysninger i offentlig forvaltning

Det er flere regelverk utover personvernregelverket som regulerer hvordan offentlig forvaltning kan bruke opplysninger.

Forvaltningsorganer er blant annet underlagt flere krav til saklighet. Det fremgår av Grunnloven § 98 annet ledd at ingen må utsettes for «usaklig eller uforholdsmessig forskjellsbehandling». Etter den ulovfestede læren om myndighetsmisbruk, som bygger på rettspraksis, gjelder det forbud mot usaklig forskjellsbehandling og mot å legge vekt på utenforliggende (usaklige) hensyn. I tillegg er det et ulovfestet krav om at offentlig forvaltning skal opptre i tråd med god forvaltningsskikk.

Det finnes også andre lover som regulerer og begrenser hva personopplysninger kan brukes til i offentlig forvaltning. For eksempel setter forvaltningslovens regler om taushetsplikt skranker for deling av opplysninger om noens «personlige forhold», dvs. av mange ulike personopplysninger. Også krav til opplysningskvalitet kan være hinder for viderebehandling av personopplysninger. Behandling for et videre formål krever for eksempel mer oppdaterte opplysninger enn det innsamlingsformålet begrunnet.

6.4 Personvernutfordringer knyttet til deling og viderebehandling av personopplysninger i offentlig forvaltning

Økt digitalisering og deling av personopplysninger i offentlig forvaltning kan på ulike måter utfordre personvernet. Det er viktig at regelverk blir fulgt, at prosesser er transparente, og at det er enkelt for innbyggerne å få informasjon om og ha oversikt over behandling av egne personopplysninger. Dette er avgjørende for at innbyggerne skal kunne ivareta rettighetene sine på en god måte.

Utfordringsbildet knyttet til deling og viderebehandling av personopplysninger i offentlig forvaltning er komplekst. I dette kapitlet trekker *Personvernkommisjonen* opp de utfordringene *kommisjonen* mener er av størst betydning, samt årsaker til disse og mulige tiltak.

Det er andre viktige utfordringer som ikke berøres i dette kapitlet, for eksempel knyttet til mangelfull bestillerkompetanse og kravsetting til innebygd personvern i de tekniske løsningene som bestilles. Utfordringer knyttet til bestillerkompetanse og leverandøroppfølging vil berøres nærmere i kapittel 8 om personvern i skolen og barnehagen.

6.4.1 Fragmentert tilnærming til personvern i offentlig forvaltning

Etter *kommisjonens* vurdering mangler det en helhetlig tilnærming til personvern i offentlig forvaltning. Per i dag har ingen offentlig virksomhet et overordnet ansvar for å vurdere den samlede bruken av personopplysninger i offentlig forvaltning. Dette resulterer i manglende helhetlig overblikk over omfanget av innsamling, bruk og videre-

[47] Personvernforordningen art. 6 nr. 4.

[48] Se mer om parlamentarisk kontroll i avsnitt 6.4.

behandling av personopplysninger i offentlig forvaltning, eller oversikt over vurderingene som gjøres når personvern veies opp mot andre hensyn.

I stor grad gjøres vurderinger knyttet til personvern i kontekst av en bestemt sektor eller et lov- eller forskriftsarbeid. Datatilsynet kan vurdere lovligheten av den enkelte behandlingsansvarliges bruk av personopplysninger, men har ikke, og bør ikke ha, ansvar for overordnede og strategiske vurderinger knyttet til personvernets stilling i forvaltningen.

Mangelen på en helhetlig tilnærming til personvern kommer til uttrykk på flere måter, og fører med seg ulike utfordringer. Nedenfor vil *kommisjonen* presentere noen av disse utfordringene, beskrive det som kan være årsaker til utfordringene og foreslå egnede tiltak.

6.4.1.1 Mangelfull koordinering av regelverksutviklingen

Personvernkommisjonen ser at en av de største utfordringene ved nødvendig deling av opplysninger mellom offentlige virksomheter ikke nødvendigvis er taushetspliktbestemmelsene, men at det mangler tilstrekkelig hjemmelsgrunnlag for å behandle opplysningene til legitime formål.

For å levere sammenhengende tjenester eller etterleve «kun én gang»-prinsippet er det viktig å se ulike sektorer og offentlige tjenester i sammenheng når regelverket utformes. På den måten kan man legge til rette for nødvendig samarbeid og eventuelt deling av opplysninger for å løse oppgaver knyttet til den sammenhengende tjenesten.

Det er behov for større grad av koordinering av regelverkutviklingsarbeidet på tvers av offentlig sektor. Mye regelverk er sektorspesifikt, og ses i begrenset grad i sammenheng med regelverk på andre områder.

Lovgiver bør i større grad sørge for å harmonisere definisjoner av begreper på tvers av regelverk. En mulighet er at disse tas inn i lovtekst som legaldefinisjoner. En annen og mer fleksibel mulighet er å klargjøre definisjoner i lovforarbeider. Begge metoder kan gjøre det lettere å se konsekvenser for personvernet av et konkret regelverk, og sammenholde disse med konsekvenser for personvernet som følge av andre relevante regelverk.

6.4.1.2 Begrenset parlamentarisk kontroll

Personvernkommisjonen mener Stortinget bør sikres større innflytelse på digitaliseringen av offentlig forvaltning og hvilke konsekvenser dette får for innbyggernes personvern. Involvering av Stortinget bidrar blant annet til at beslutninger blir bedre belyst og får bredere forankring.

Personvernkommisjonen mener det i dag er et problem at for mange tiltak med stor innvirkning på innbyggernes personvern forskriftsfestes, i stedet for at de hjemles i lov og blir en sak Stortinget må ta stilling til. På den måten mister Stortinget muligheten til å ha oversikt over bruken av personopplysninger i forvaltningen. Dette henger tett sammen med avsnitt 6.4.2 om vide hjemler.

Personvernkommisjonen mener offentlig forvaltning har et særlig ansvar for å ivareta befolkningens tillit. Dette krever grundige vurderinger av om formålet med viderebehandlingen av innbyggernes personopplysninger er forenelig eller ikke med det opprinnelige innsamlingsformålet og hvor stort inngrep viderebehandlingen innebærer. Disse vurderingene bør offentliggjøres. Hvilke vurderinger som bør gjøres omtales under rettslige rammer i avsnitt 6.3.

6.4.1.3 Mulige årsaker til mangelen på helhetlig tilnærming

Personvernkommisjonen vil i det følgende peke på noen mulige årsaker til utfordringene som er beskrevet over.

Manglende personvernpolitikk

Det er ikke utviklet en helhetlig politikk for personvern. Politikken på området er delvis gitt på europeisk nivå, gjennom utformingen av personvernforordningen. Hvordan det nasjonale handlingsrommet som forordningen åpner for benyttes, bør være gjenstand for mer systematisk og helhetlig debatt, som beskrevet i kapittel 10. Det er behov for å løfte diskusjonen om nye hjemler for deling eller bruk av personopplysninger fra å handle om konkrete og isolerte endringer på ett område, til å også bli en åpen samfunnsdebatt om verdier og prinsipper.

På vei mot en mer datadrevet forvaltning vil man støte på mange muligheter som, selv om de er lovlige ut fra gjeldende rett, kan være etisk utfordrende. At det er lov å dele og viderebehandle personopplysninger betyr ikke nødvendigvis at det skal eller bør gjøres. Innhenting, bruk og viderebehandling av personopplysninger kan komme i konflikt med etiske og moralske normer i samfunnet eller utfordre grunnleggende samfunnsmessige verdier og prinsipper. Diskusjonen om hvordan personvern skal vektes opp mot andre viktige hensyn bør skje i form av åpen

debatt og er verdispørsmål som bør avgjøres på politisk nivå.

En effektiv forvaltning er viktig, blant annet for å sikre gode innbyggertjenester. *Personvernkommisjonen* ønsker imidlertid å advare mot å vektlegge effektivitet så tungt at det går ut over den enkelte innbygger sine grunnleggende rettigheter og friheter, herunder retten til personvern.

Personvernkommisjonen etterlyser en åpen debatt om veiing av kryssende hensyn mellom personvern og andre hensyn, som for eksempel effektivisering. *Kommisjonen* savner en beskrivelse av *hvordan* forvaltningsorganer skal vektlegge spørsmål om personvern, og hvordan disse vurderingene skal gjennomføres.

Personvernkommisjonen ser det som nødvendig med en personvernpolitikk som kan balansere digitaliseringspolitikken. Digitaliseringspolitikken er ambisiøs på vegne av offentlig forvaltning, men tar etter *kommisjonens* syn ikke tilstrekkelig høyde for at realisering av politikken forutsetter lovendringer.

Personvernkommisjonen vil fremheve behovet for at regjeringen utarbeider en helhetlig personvernpolitikk for offentlig forvaltning, som ses i sammenheng med digitaliseringspolitikken og gir føringer for hvordan forvaltningen skal gjøre prinsipielle vurderinger om personvern og sikre at borgernes personvern ivaretas i løsningene som utvikles. I personvernpolitikken bør regjeringen ha særlig oppmerksomhet på personvernkonsekvensene av mer utstrakt deling og viderebehandling av personopplysninger, og hvordan disse skal vurderes opp mot andre viktige hensyn som effektivisering og rettsikkerhet.

Personvernkommisjonen anbefaler at regjeringen legger frem en personvernpolitisk redegjørelse for Stortinget årlig, forankret i gjeldende personvernpolitikk.

Mangel på helhetlig overblikk

I dag har ingen virksomhet i offentlig forvaltning et dedikert ansvar for å jobbe helhetlig og horisontalt med personvern. Som et neste steg etter utviklingen av en personvernpolitikk, kan det være naturlig å se på om det er behov for en funksjon eller virksomhet med ansvar for gjennomføring av politikken.

Vurderinger knyttet til innsamling, deling og bruk av personopplysninger foretas i stor grad sektorvis, med varierende grad av parlamentarisk kontroll og ofte uten åpen debatt. I tillegg til en funksjon som nevnt over, mener *Personvernkommisjonen* det er et behov for et rådgivende og frittstående organ for forvaltningen som kan vurdere og drøfte prinsipielle og generelle spørsmål knyttet til bruk av personopplysninger i offentlig forvaltning, herunder samfunnsmessige og etiske spørsmål. I Danmark har regjeringen opprettet et Dataetisk råd som skal gi råd og innspill til regjeringen, Folketinget og offentlige myndigheter om dataetiske spørsmål ved bruken av data og ny teknologi. Rådet skal også bidra til å understøtte en kultur i offentlig forvaltning for ansvarlig bruk av personopplysninger.[49]

Et slikt organ i Norge kan blant annet:

- Legge stor vekt på informasjons- og debattskapende aktiviteter ved å bidra til informasjon til publikum og bidra til kommunikasjon mellom offentlige myndigheter, fagfolk og interesseorganisasjoner.
- Gi uttalelser i saker om lovregulering av bruk av personopplysninger i offentlig forvaltning og digitaliseringstiltak som har betydning for personvern, etter begjæring eller av eget initiativ.
- Gi uttalelser til norske myndigheter i spørsmål om personvern og digitalisering i internasjonale organer.
- Offentliggjøre sine uttalelser med mindre annet følger av lovbestemt taushetsplikt.

6.4.2 Utforming av lovhjemler

Utfordringene knyttet til en manglende helhetlig tilnærming til bruk av personopplysninger i offentlig forvaltning henger tett sammen med utfordringer på et lavere nivå knyttet til spesifikke regelverksarbeid.

6.4.2.1 Manglende vurdering av personvernkonsekvenser i lovarbeid

Utredningsinstruksen[50] forutsetter utredning av konsekvenser ved ulike tiltak. Konsekvensutredninger er sentralt ved alt regelverksarbeid. Utredningsinstruksen skal sikre at det alltid foretas utredninger som omfatter «virkninger for enkeltpersoner privat og offentlig næringsvirksomhet, statlig, fylkeskommunal og kommunal forvaltning

[49] Justitsministeriet. (u.å). *Dataetisk råd.*

[50] Utredningsinstruksen ble første gang fastsatt ved kongelig resolusjon 18. februar 2000 og er revidert i 2005 og 2016. Den gjeldende instruksen ble fastsatt ved kongelig resolusjon 19. februar 2016, med virkning fra 1. mars 2016. Formålet med utredningsinstruksen er å legge et godt grunnlag for beslutninger om statlige tiltak, som for eksempel reformer, regelendringer og investeringer. Finansdepartementet. (2016). *Utredningsinstruksen*.

og andre berørte». Personvernkonsekvenser kan være en type konsekvenser som skal vurderes ved lovarbeid. Det finnes egne tilleggsveiledninger til Utredningsinstruksen om for eksempel konsekvenser for likestilling, næringsøkonomiske konsekvenser, *personvernkonsekvenser* og miljøutredninger. Det følger av Utredningsinstruksen med tilleggsveileder at det i lovarbeid skal utredes hvilke konsekvenser lovforslaget kan ha for personvern, der det er relevant. Vurderingene av personvernkonsekvenser skal utredes som ledd i den ordinære utredningsprosessen.

Personvernforordningen stiller også klare krav til utredning av personvernkonsekvenser. Der Utredningsinstruksen er generell, er personvernforordningen mer konkret om *når* det skal gjøres konsekvensvurderinger, og også *hva* som skal vurderes. Se nærmere i kapittel 4 om vurderinger av personvernkonsekvenser etter *personvernforordningen*.

Vurderingen av personvernkonsekvenser i lovarbeid er avgjørende for å kunne bedømme hvilken påvirkning loven vil ha på personvernet. Det er også en forutsetning for parlamentarisk kontroll og domstolskontroll. Inngrep i personvernet må skje innenfor rammene EMK artikkel 8 og Grunnloven § 102 oppstiller. Det er viktig å vurdere om, og dokumentere at, de inngrepene som gjøres er nødvendige og forholdsmessige.

Vurderinger av personvernkonsekvenser er viktig for å sikre åpenhet om hvordan forvaltningen vektlegger og balanserer personvernhensyn i møte med andre hensyn og verdier. Det er også nødvendig for å kunne vurdere om det bør lovfestes tiltak som skal avhjelpe konsekvensene, og for vurderingen av hvorvidt disse tiltakene er egnede og tilstrekkelige. Når konsekvensene for personvernet som følge av lovforslag ikke vurderes godt nok, blir det også vanskelig å få oversikt over de samlede konsekvensene for personvernet av flere lovvedtak.

Personvernkommisjonen mener vurdering av personvernkonsekvenser i lovarbeid bør inkludere vurderinger av om eksisterende regelverk er tilstrekkelig og om det nasjonale handlingsrommet i personvernforordningen artikkel 6 nr. 3 skal anvendes. Bestemmelsen i personvernforordningen artikkel 6 nr. 3 omfatter tilfeller der behandlingsgrunnlag for behandling av personopplysninger finnes i artikkel 6 nr. 1 bokstav c («rettslig forpliktelse») og bokstav e («oppgave i allmennhetens interesse» og «utøve offentlig myndighet»). Dersom det fastsettes nasjonale bestemmelser, kan dette bidra til klarere og mer utfyllende regelverk, og dermed gi større forutberegnelighet for innbyggerne. Det vil også gi bedre grunnlag for å vurdere lovligheten av konkrete behandlinger av personopplysninger.

6.4.2.2 Vide hjemler

Sett fra et digitaliseringsvennlig ståsted, vil vidt utformede lovhjemler i mange sammenhenger kunne fremstå som fordelaktig. Det gir forvaltingsorganene rom til å vurdere hvilke behandlingsaktiviteter som er mest relevante for en effektiv og god oppgaveløsning. Samtidig gir fleksible lovreguleringer også redusert behov for tid- og ressurskrevende regelverksarbeid.

På den andre siden reduserer denne lovteknikken den parlamentariske kontrollen i regelverksutviklingen, og vid utforming av lovbestemmelser vil gi mindre forutsigbar praksis. Utstrakt bruk av vidt utformede regler vil også øke risikoen for at innhenting, sammenstilling og viderebruk av personopplysninger samlet sett overstiger et ønsket og håndterbart nivå.

Personvernregelverket, legalitetsprinsippet, Grunnloven § 102 og EMK artikkel 8, stiller krav til rettslig grunnlag for behandlingen av personopplysninger, og hvordan dette bør utformes. Det må gjøres vurderinger og avgrensninger i forarbeidene, og mer detaljerte vilkår bør følge av forskrift hvis det ikke er mulig å være presis i selve loven. Jo mer inngripende behandlingen er, jo strengere er kravet til klarhet og presisjon.

6.4.2.3 Særlig om profilering

Når forvaltningen benytter seg av profilering eller tar avgjørelser som er basert på helautomatisert behandling av personopplysninger, kommer personvernforordningen artikkel 22 til anvendelse. Bestemmelsen er ikke begrenset til formelle avgjørelser eller til enkeltvedtak etter forvaltningsloven, men omfatter også avgjørelser som «på tilsvarende måte i betydelig grad påvirker vedkommende». Mona Naomi Lintvedt[51] peker i sin utredning på at prosessledende avgjørelser, som for eksempel utplukk til kontroll, kan være av en så inngripende karakter at det vil kunne ha tilsvarende betydning for den registrerte som en «avgjørelse».[52] Når artikkel 22 kommer til anvendelse må den behandlingsansvarlige kunne vise til et supplerende rettslig grunnlag i nasjonalretten. Det må derfor vurderes hvilken betydning offent-

[51] Lintvedt, M. N. (2022). *Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering*. Utredning for Personvernkommisjonen.

Boks 6.3 Eksempel: Forvaltningslovens § 13g

Forvaltningsloven (fvl.) § 13g kan tjene som eksempel både på manglende personvernkonsekvensvurderinger og vide hjemler. Bestemmelsen åpner for større adgang til å dele taushetsbelagte opplysninger mellom forvaltningsorganer, herunder personopplysninger, enn tidligere. En slik endring av lovverket har klare personvernimplikasjoner. Dermed må lovgiver vurdere personvernskonsekvensene av forslaget.

I forarbeidene utreder Justisdepartementet kravene til utformingen av lovregelen i tråd med Grunnloven og EMK og kravene til supplerende rettsgrunnlag etter personvernforordningen. Departementet vurderer dermed *formelle vilkår for lovligheten* av lovforslaget sett i lys av personvernforordningens rammer.[1] Det vil si om det er adgang etter forordningen til å vedta en slik lov. Justisdepartementet vurderte imidlertid ikke hvilke *konsekvenser* lovforslaget har for innbyggernes personvern.

Forvaltningsloven § 13g åpner for at det kan gis forskriftshjemler om deling av opplysninger mellom offentlige virksomheter. Et eksempel på dette er forskrift om a-krimsamarbeidet[2] som vil gjøre det mulig for de involverte virksomhetene å dele opplysninger innenfor rammene av samarbeidet for å forebygge og bekjempe arbeidslivskriminalitet.

Lovhjemmelen i fvl. 13g er vid og lite spesifikk, mens detaljene for den konkrete delingen fastsettes i forskrift.

1 Prop. 166 L (2020–2021) *Endringer i forvaltningsloven m.m. (utvidet adgang til informasjonsdeling)*. s. 21.

2 Justis- og beredskapsdepartementet. (2021). *Høring om forslag til forskrift om deling av taushetsbelagte opplysninger og behandling av personopplysninger m.m. i det tverretatlige samarbeidet mot arbeidslivskriminalitet.*

lige virksomheters bruk av automatisert behandling og/eller profilering har for den registrerte.

Det er uheldig at hver enkelt etat foretar disse vurderingene hver for seg. Det ville bidra til klarhet hvis vurderingen av om en avgjørelse har rettsvirkning eller tilsvarende betydning ikke overlates til hver etat, men heller ble vurdert i lov- og forskriftsarbeidet.

Vide hjemler vil i stor grad overlate balanseringen av personvernhensyn mot andre relevante hensyn, så som kontrollhensyn, til den enkelte etat. Etatene må også foreta vurderinger av om profilering støter an mot diskrimineringsforbudet eller god forvaltningsskikk. *Personvernkommisjonen* mener slike vurderinger i langt større grad enn i dag må gjøres kjent for offentligheten.

6.4.2.4 *Mulige årsaker til mangler i regelverksutviklingen*

Det kan være flere årsaker til at det ikke tas tilstrekkelig hensyn til personvern i regelverksutviklingen. *Personvernkommisjonen* vil her peke på utilstrekkelig veiledning, mangel på kompetanse og ressurser og mangelfull etterlevelse av plikten til å rådføre seg med Datatilsynet, jf. personvernforordningen artikkel 36 nr. 4, som mulige årsaker.

Utilstrekkelig veiledning

Arbeidet med lov- og forskrifter skal som nevnt gjøres i tråd med *Utredningsinstruksen*.[53] Instruksen skal sikre at statlige beslutninger er velbegrunnede og gjennomtenkte.

I 2008 ble det utgitt en tilleggsveileder til utredningsinstruksen om *vurdering av personvernkonsekvenser.* Målet var å lette forståelsen av i hvilke saker det var nødvendig å vurdere personvernkonsekvenser, når i prosessen dette skulle gjøres, og hvordan vurderingene skulle gjøres. Veilederen ble utarbeidet for å ivareta krav i den tidligere (nå opphevede) personopplysningsloven. *Personvernkommisjonen* har fått opplyst at veilederen nå er under oppdatering i Kommunal- og distriktsdepartementet.

Personvernkommisjonen ser det som svært positivt at det er igangsatt et arbeid i departementet med å oppdatere veilederen.

Personvernkommisjonen mener det er nødvendig å få på plass en forståelig og anvendelig veile-

52 EDPB har gitt sin tilslutning til Artikkel 29-gruppens uttalelser hvor denne problemstillingen er nærmere beskrevet. Article 29 Working Party. (2018). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.*

53 Finansdepartementet. (2016). *Utredningsinstruksen*.

der for vurdering av personvernkonsekvenser i lov- og forskriftsarbeid. Veilederen bør legge til rette for at ansvarlig departement kan synliggjøre både personvernkonsekvensene av det tiltaket som innføres isolert sett, og de samlede personvernkonsekvensene av ulike tiltak som allerede er på plass på det aktuelle området.

I tillegg til en ny veileder om vurderinger av personvernkonsekvenser til utredningsinstruksen, mener *Personvernkommisjonen* at også veilederen om lovteknikk- og lovforberedelse («lovteknikkheftet») bør oppdateres.[54] Lovteknikkheftet er ikke oppdatert hverken med henvisninger til dagens utredningsinstruks, veileder for digitaliseringsvennlig regelverk eller den oppdaterte tilleggsveilederen om vurderinger av personvernkonsekvenser.

Utilstrekkelig kompetanse og ressurser

Kompetanseheving og opplæring i personvern er et lederansvar og et krav i personvernregelverket. *Personvernkommisjonen* har inntrykk av at det er bygget opp betydelige kompetansemiljøer på personvern i store deler av forvaltningen de siste årene. Den silo-orienterte oppbygningen av offentlig sektor bidrar imidlertid til små miljøer som sitter adskilt fra hverandre, og kompetansemiljøene drar i liten grad synergieffekter av hverandres kunnskap og innsikt. Dette gjelder alt fra lov- og forskriftsuforming til juridiske vurderinger knyttet til utvikling av konkrete løsninger.

Den digitale utviklingen i offentlig forvaltning og samfunnet for øvrig, gjør at det stadig oppstår nye juridiske problemstillinger og avklaringsbehov knyttet til hvordan ny teknologi eller nye behandlingsprosesser påvirkes av personvernregelverket. Dette er dynamiske og vedvarende prosesser der kompetanse, kunnskap og innsikt utvikles kontinuerlig.

Mange av problemstillingene er likelydende for store deler av offentlig forvaltning. For eksempel har Schrems II-dommen pekt på juridiske problemstillinger knyttet til bruk av mange digitale tjenester, som vil gjelde på tvers av forvaltningen. Et annet eksempel er kompetanse knyttet til lovlig og etisk bruk av kunstig intelligens i offentlig forvaltning. For slike tilfeller bør det legges opp til felles kompetanseheving og utvikling av «beste praksis» og veiledning. Eksempelvis kan dokumenterte og publiserte resultater fra Datatilsynets sandkasse for kunstig intelligens[55] gjøre det mulig for mange virksomheter å dra nytte av andres pilotarbeid. Videre er «Koordineringsarbeidet etter Schrems II» et eksempel på hvordan virksomheter i offentlig forvaltning kan samarbeide for å sikre faglig kvalitet og god ressursbruk i krevende og likelydende juridiske vurderinger.[56]

Personvernkommisjonen anbefaler at offentlig forvaltning styrker personvernkompetansen til ledere, saksbehandlere og andre ansatte som har behov for slik kompetanse. I arbeidet med regelverksutvikling bør det stilles krav til personvernkompetanse. Kunnskap om personvern bør inngå i den obligatoriske grunnopplæringen til nyansatte saksbehandlere, på lik linje med opplæring i forvaltningsloven og offentleglova.

Rådføringsplikten med Datatilsynet i lov- og forskriftsarbeid

Personvernforordningen artikkel 36 nr. 1 hjemler en plikt for den *behandlingsansvarlige* til å rådføre seg med Datatilsynet dersom de tar sikte på å igangsette en behandling av personopplysninger som kan medføre høy risiko for de registrertes personvern. En lignende plikt til å rådføre seg med tilsynsmyndigheten gjelder etter personvernforordningen artikkel 36 nr. 4:

> «Medlemsstatene skal rådføre seg med tilsynsmyndigheten ved utarbeiding av forslag til lovgivning som skal vedtas av et nasjonalt parlament, eller av et reguleringstiltak som er basert på slik lovgivning, og som er knyttet til behandling.»[57]

Personvernkommisjonen mener artikkel 36 nr. 4 forutsetter en særskilt rådføringsplikt. Bestemmelsen kan ikke anses å være etterlevet ved å gi Datatilsynet anledning til å være høringsinstans i forbindelse med en ordinær offentlig høringsprosess. I alle tilfeller påligger det regjeringen å utrede lovgivning så omfattende og grundig som nødvendig, og på balansert, systematisk og helhetlig måte når spørsmålene er av prinsipiell karakter. Dersom Datatilsynet involveres på et tidlig tidspunkt kan tiltakets nødvendighet belyses, og det er mulig å drøfte utforming av ulike virkemidler for å sikre at personvernet blir ivaretatt etter at loven har trådt i kraft. Rådføringsplikten,

[54] Justisdepartementet. (2000). *Lovteknikk og lovforberedelse: Veiledning om lov og forskriftsarbeid*.

[55] Datatilsynet. (2022). *Sandkassesiden*.

[56] Digitaliseringsdirektoratet. (u.å). *Koordinering av arbeidet med Schrems II-dommen*.

[57] Personvernforordningen art. 36 nr. 4.

og hvordan *kommisjonen* mener den bør forstås og innrettes, diskuteres i kapittel 13. Rådføringsplikten er også omtalt i kapittel 7.

Personvernkommisjonen anbefaler at regjeringen vurderer om rådføringsplikten etter personvernforordningen følges i tilstrekkelig grad i dag. En slik vurdering bør også inneholde vurderinger av hvordan rådgivningsplikten kan innrettes for å ikke forsinke lovarbeidet, samt føre til en uforholdsmessig stor ressursbelastning for Datatilsynet. Disse vurderingene bør gjøres som ledd i utviklingen av en personvernpolitikk.

6.4.3 Deling av personopplysninger mellom forvaltningsorganer

Offentlige organer har behov for å utveksle opplysninger på tvers av virksomheter for å løse oppgaver og for å utvikle og forbedre saksbehandlingen og tjenester rettet mot innbyggerne. Slik deling vil ofte innebære at personopplysninger også viderebehandles til formål som ikke er forenlige med det formålet de opprinnelig ble innsamlet for.

Et eksempel er at UDI mottar informasjon fra politiet om brudd på straffeloven eller utlendingsloven, som grunnlag for vurdering i utvisningssaker. Et annet eksempel er at Skatteetaten deler informasjon om inntektsopplysninger med Husbanken så de kan saksbehandle lånesøknader.

Virksomheter kan også inngå større samarbeid der deling av opplysninger er en sentral og vesentlig del av samarbeidet. Et eksempel er Tilda, en løsning som skal sikre god informasjonsflyt mellom tilsynsmyndighetene i Norge, og der målet er koordinerte, effektive og mer målrettede tilsyn.[58]

Behovet for deling av opplysninger mellom offentlige virksomheter er omtalt i Digitaliseringsstrategien, som oppfordrer til deling av data på tvers av forvaltningsorganer.

> «Gjenbruk av informasjon bidrar til raskere og enklere saksgang både for brukerne og for de offentlige virksomhetene. Offentlige virksomheter skal ikke spørre brukerne på nytt om forhold de allerede har opplyst om. Dette omtales gjerne som «kun én gang», og er et langsiktig mål og en av hovedprioriteringene i IKT-politikken. Finnes data hos en annen virksomhet, skal data hentes derfra, forutsatt at det foreligger rettslig grunnlag. Dette er også fastsatt i Digitaliseringsrundskrivet punkt 1.2.
>
> Utvekslingen skal skje på en måte som bevarer dataenes autentisitet og integritet. Utveksling av data som andre offentlige virksomheter har krav på, skal prioriteres.»

Trygg og effektiv deling av data mellom offentlige myndigheter forutsetter at aktørene gjør grundige og forsvarlige juridiske vurderinger. Vurderingene kan være krevende. En av grunnene er at vurderingene berører flere regelverk som må sees i sammenheng, herunder personvernregelverket, og innebærer vekting av flere hensyn. En annen grunn er at faktum, den virkeligheten rettsreglene skal vurderes mot, ofte innebærer avanserte teknologiske løsninger. For å hjelpe virksomheter med de krevende vurderingene er det opprettet et Nasjonalt ressurssenter for deling og bruk av data (Digdir) som skal veilede om problemstillinger knyttet til deling av data.[59]

6.4.3.1 Uklare roller og ansvar i samarbeid der det deles personopplysninger

En utfordring ved deling av personopplysninger på tvers av organer, er at det oppstår usikkerhet rundt *ansvarsforholdet* mellom samarbeidende organer. For å sikre at de registrertes rettigheter ivaretas på en god og hensiktsmessig måte, er det viktig å klargjøre behandlingsansvaret mellom behandlingsansvarlige virksomheter. For eksempel hvorvidt det kan sies å foreligge et databehandlerforhold,[60] eller om det kan være felles behandlingsansvar.[61]

Det eksisterer mange ulike og til dels kompliserte samarbeidsformer som gjør at rolleavklaringen ikke alltid er like åpenbar. Det kan være nødvendig å fastsette forskriftshjemler i flere særlover for å dekke et bestemt behov for informasjonsdeling.

Fordeling av roller og ansvar kan gjøres i lov- eller forskriftshjemmel for samarbeidet, dersom samarbeidet er hjemlet i lov eller forskrift, jf. personvernforordningen artikkel 4 nr. 7.[62]

Personvernkommisjonen anbefaler at ansvarsfordelingen i større grad bør lov- eller forskriftsfestes der deling av personopplysninger inngår

---

58 Brønnøysundsregistrene. (2021). *Enklere deling av tilsynsdata med Tilda*.

59 Digitaliseringsdirektoratet. (u.å). *Fordeling av roller og ansvar når dere skal dele data*.

60 Se personvernforordningen art. 4 nr. 8.

61 Se personvernforordningen art. 4 nr. 7.

62 Se for eksempel Helse- og omsorgsdepartementet. (2021). *Høringsnotat om endringer i pasientjounalloven*. Punkt 5-5-3.

som en del av et større samarbeid mellom forvaltningsorganer og hvor uklarhet kan medføre alvorlige personvernkonsekvenser. Særlig er dette aktuelt der det er snakk om mer komplekse samarbeid. Dette vil føre til klarhet og gi større bevissthet om forpliktelser knyttet til behandlingsansvaret hos det enkelte organ. For eksempel kan det reguleres hvem som er ansvarlig for informasjonssikkerhet der samarbeidet innebærer bruk av felles tekniske løsninger. Videre kan det reguleres hvem som er ansvarlig for informasjonsplikten og andre plikter, noe som vil styrke den registrertes rettigheter. Samtidig vil forvaltningsorganene unngå å bruke ressurser på å utrede hvilket organ som har ansvar for hva.

Den nasjonale adgangen til å skape klarhet i ansvarsplasseringen, slik forordningen åpner for, er nærmere diskutert i kapittel 10.

Personvernkommisjonen mener det må utarbeides og videreutvikles standarder for deling av personopplysninger. Dette gjør det lettere å samarbeide, og bidrar til å sikre høyere faglig kvalitet og effektiv ressursbruk.

Deling av taushetsbelagte opplysninger i mottakers interesse

Det finnes en rekke bestemmelser som åpner opp for adgang til å dele taushetsbelagte opplysninger i de tilfellene hvor det er i mottakerorganets interesse at opplysningene deles.[63] Dette forutsetter at partene på hver sin side har nødvendig behandlingsgrunnlag for å behandle opplysningene, som kan være nedfelt i sektorspesifikk særlov. Det er avgiverorganet som har taushetsplikt og dermed må vurdere hvorvidt vilkårene for deling er oppfylt, i dette tilfeller om mottakerorganet har behov for opplysningene for å utføre sine lovpålagte oppgaver. I tilfellet hvor behandlingsgrunnlaget for mottakerorganet er regulert i særlov, synes det ofte å være en utfordring for avgiverorganet å klargjøre om mottakerorganet har behov for opplysningene, og dermed behandlingsgrunnlag for å få dem utlevert.

6.4.3.2 Ivaretakelse av den registrertes rettigheter ved deling av data

Det offentlige består av mange behandlingsansvarlige som har ansvar for den behandlingen av personopplysninger som faller under egen oppgaveløsning. Utveksling av opplysninger mellom behandlingsansvarlige kan gjøre det utfordrende å holde oversikt over dataflyten. Gode automatiserte løsninger kan bidra til å avhjelpe dette. For innbyggerne kan det likevel være vanskelig å vite hvilken behandlingsansvarlig de skal forholde seg til for å håndheve sine rettigheter etter personvernforordningens kapittel III.

Underrettingsplikten artikkel 19

Personvernforordningen artikkel 19 pålegger den behandlingsansvarlige en underrettingsplikt og skal sikre at den enkeltes rettigheter blir ivaretatt når personopplysningene deres deles videre med andre virksomheter. Forvaltningsorganet som har innhentet og delt innbyggernes personopplysninger med andre virksomheter, plikter å underrette mottakervirksomheten dersom personopplysningene senere har blitt rettet, slettet, eller har blitt gjenstand for begrenset behandling.[64]

Økt datadeling kombinert med manuelle rutiner for underretting, kan være krevende å gjennomføre i praksis. Dette kan igjen medføre at underrettingsplikten ikke blir tilstrekkelig ivaretatt. Digitalisering og automatiske løsninger for deling av data gir imidlertid også muligheten for å automatisk underrette, rette eller slette hos virksomheter som har mottatt opplysninger fra den opprinnelige behandlingsansvarlige.

Krav til datakvalitet og informasjonsbehandling

Personvernforordningen fastsetter et prinsipp om at personopplysningene som inngår i en behandling skal være korrekte.[65] Kravet til riktighet er av relativ karakter; det går fram av prinsippet at hvorvidt opplysningene er tilstrekkelig korrekte, må vurderes i lys av formålene opplysningene skal behandles for. Det betyr at personopplysninger som tilfredsstiller kravet til korrekthet i én behandling, ikke nødvendigvis vil være tilstrekkelig korrekte for behandling til et annet formål.

Når personopplysninger viderebehandles, og særlig når dette skjer til formål som er uforenlige med det opprinnelige formålet, oppstår en risiko for at personopplysningene ikke er tilstrekkelig korrekte for å oppfylle formålene med den nye behandlingen.

Det er den behandlingsansvarlige som må vurdere om personopplysningene som innhentes til et formål innehar tilstrekkelig datakvalitet. Der

[63] Se for eksempel Lov 27. mai 2016 nr. 14 om skatteforvaltning, (skatteforvaltningsloven) § 3-3 (1) eller forvaltningsloven § 13 bokstav g.

[64] Se personvernforordningen art. 19.

[65] Se personvernforordningen art. 5 nr. 1 bokstav d.

slik deling skjer mellom forskjellige behandlingsansvarlige virksomheter, blir det imidlertid særlig viktig at datakvaliteten beskrives godt hos avgiverorganet, slik at mottaker blir satt i stand til å vurdere om opplysningene holder tilstrekkelig kvalitet for den nye behandlingen de skal inngå i. Slike beskrivelser krever godt og systematisk arbeid med informasjonsforvaltning. Informasjonsforvaltning er et viktig og ressurskrevende arbeid, som *Personvernkommisjonen* mener bør styrkes og prioriteres.

Krav til dataminimering

Personvernforordningen oppstiller et prinsipp om at den behandlingsansvarlige ikke skal behandle flere personopplysninger enn det som er nødvendig for å oppnå formålet med behandlingen. Personopplysningene som inngår i en behandling skal, ifølge forordningen, være «adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for».[66]

Bruk av fingranulerte løsninger der det er dataelementer heller enn hele dokumenter som deles, gjør det mulig å utveksle opplysninger på en måte som ivaretar plikten til dataminimering. Løsningen *Samtykkebasert lånesøknad*[67] kan tjene som eksempel. Istedenfor at den registrerte leverer hele skattemeldingen til banken, som inneholder langt flere opplysninger enn det banken har behov for i søknadsbehandlingen, kan den registrerte samtykke til at banken innhenter forhåndefinerte datasett direkte fra Skatteetaten. Banken innhenter således bare de opplysningene som er nødvendige for formålet de skal benyttes til.

På den andre siden kan en situasjon der forvaltningen innhenter opplysninger fra en annen virksomhet, i stedet for fra den registrerte selv, i seg selv innebære en risiko for at det organet som tilbyr opplysningene, får informasjon som kan indikere at en person for eksempel er i kontakt med helsevesenet, Nav eller andre etater. Det genereres altså en personopplysning om den registrerte som dette organet ikke har bruk for i sin egen oppgaveløsning, og som virksomheten heller ikke ville hatt dersom den registrerte selv leverte opplysningene til mottakerorganet. Den negative konsekvensen av dette kan i noen grad reduseres ved at delingen skjer automatisk/maskinelt, uten at en saksbehandler er direkte involvert og ser hvor opplysninger om en bestemt person er hentet fra. Dette vil imidlertid ikke avhjelpe det faktum at opplysningene vil befinne seg i avgiverorganets utleveringslogg.

En alternativ løsning som kan gi den registrerte økt innflytelse og medbestemmelsesrett i forbindelse med behandlingen, er å åpne for at den registrerte selv samtykker til hvorvidt opplysningene skal hentes fra en annen virksomhet, eller om den registrerte ønsker å fremskaffe dokumentasjon selv. *Personvernkommisjonen* mener det bør foretas en vurdering av hvilket handlingsrom personvernforordningen gir for denne type samtykkebasert deling, og hvorvidt det er ønskelig at offentlige virksomheter tilrettelegger for dette.

Retten til informasjon og til å kreve innsyn

Det er et klart uttalt politisk mål at det offentlige Norge i økende grad skal tilby sammenhengende tjenester. Et av kjennetegnene ved slike tjenester er at det ikke er synlig for brukeren at tjenesten, og dermed personopplysninger, flyter gjennom ulike forvaltningsnivåer og forskjellige siloer. Tjenestene skal oppleves som sømløse og sammenhengende, og brukeren skal slippe å forholde seg til forvaltningens interne organisering.[68]

For at den registrerte skal kunne utøve sin rett til for eksempel innsyn, retting eller sletting, er det viktig å sikre at innbygger har reell mulighet til å orientere seg om hvilken behandling som skjer og hvilken virksomhet som er behandlingsansvarlig. Det vil derfor være nødvendig at de ulike behandlingene, med tilhørende behandlingsansvarlige virksomheter, som inngår i de sammenhengende tjenestene synliggjøres for innbyggeren. God etterlevelse av informasjonspliktene etter personvernforordningen artikkel 12, 13, 14 og 15 blir derfor av stor betydning for at den registrerte har reelle muligheter til å kreve sine rettigheter oppfylt. Åpenhet og informasjon om hvordan offentlige virksomheter behandler personopplysninger er også viktig for å ivareta innbyggernes tillit til myndighetene.

Digitalisering kan gi gode forutsetninger for å utvikle automatiserte løsninger for å håndheve rettigheter. Blant disse er automatiserte innsynsløsninger.

Digitaliseringsdirektoratet har på oppdrag av Kommunal- og distriktsdepartementet utredet muligheten for innsyn i personopplysninger. Direktoratet har gjennomført en mulighetsstudie med

---

66 Se personvernforordningen art. 5 nr. 1 bokstav c.

67 Altinn utvikling. (u.å.). *Samtykkebasert lånesøknad*.

68 Kommunal- og distriktsdepartementet. (2019). *Én digital offentlig sektor: Digitaliseringsstrategi for offentlig sektor 2019-2025*. Kapittel 2.

mål om å identifisere innsatsområder og tiltak som kan sikre at innbyggerne får oppfylt rettighetene sine etter personvernregelverket. Rapporten fra Digitaliseringsdirektoratet ble publisert i juni 2022. I rapporten foreslår direktoratet flere konkrete tiltak, fordelt over tre innsatsområder, som sammen gir et fundament for videre arbeid med løsninger for innsyn og kontroll. Det første innsatsområdet gjelder oversikt over personopplysninger. Digitaliseringsdirektoratet peker på at innbyggerne må vite hvem man kan henvende seg til, og om hva, for å være i stand til å kreve innsyn etter personvernforordningen. I tillegg vises det til at mange også spør om generell informasjon om hvordan det offentlige behandler og deler personopplysninger, heller enn et konkret innsyn i egne personopplysninger. God oversikt kan derfor bidra til en forståelse som gjør at innsyn ikke alltid er nødvendig. Tiltakene som foreslås skal bidra til økt åpenhet rundt behandling av personopplysninger gjennom å gi innbyggerne oversikt over hvilke personopplysninger som behandles, og hvor i offentlig sektor behandling skjer.

Veiledning og innsyn for innbygger er det andre innsatsområdet. Digitaliseringsdirektoratet erfarer at hverken innbyggere eller virksomheter alltid vet hvor man skal henvende seg eller hvilken type innsyn som passer best til situasjonen. Digitaliseringsdirektoratet foreslår et tiltak for å samle veiledning og muligheten til å be om innsyn på ett sted, og på den måten sette innbyggeren i sentrum. I den sammenheng forelås det videre å etablere en standard for hvordan offentlige virksomhter skal håndtere innsyn.

Det tredje innsatsområdet gjelder innbyggernes tilgang til egne personopplysninger. Formålet med disse tiltakene er økt datadeling gjennom å gi innbyggerne tilgang til å bruke egne opplysninger. Et forslag er å definere et sett med kjerneopplysninger som innbygger har varierende grad av råderett over, som førerkort, vitnemål eller inntektsopplysninger.

Digitaliseringsdirektoratets utredning om innsyn og kontroll med hvordan personopplysninger behandles i offentlige virksomheter er svært grundig og god og tiltakene som foreslås treffer godt. *Kommisjonen* anbefaler at Kommunal- og distriktsdepartementet følger opp utredningen i arbeidet med å tilrettelegge for god ivaretakelse av innbyggernes rettigheter i offentlig forvaltning. Utredningen vil kommenteres ytterligere i kapittel 12, der det refereres til de foreslåtte tiltakene i sin helhet.

6.4.4 Bruk av kunstig intelligens

Personvernkommisjonen anerkjenner at bruken av kunstig intelligens, herunder maskinlæring i forvaltningen kan være et viktig verktøy som bidrar til gode og effektive løsninger. Bruken reiser samtidig en rekke utfordringer knyttet til behandling av store mengder personopplysninger, manglende transparens og kompleksitet, som kommentert i avsnitt 6.2.3.

Personvernkommisjonen mener lovregulering av bruk av kunstig intelligens bør ha som formål å motvirke maktubalansen mellom offentlig forvaltning og innbyggerne. Jo mer inngripende behandlingen er, dess større krav bør en stille til åpenhet og andre rettsikkerhetsmekanismer. Med rettssikkerhetsmekanismer menes regler som er essensielle for å ivareta borgernes rettssikkerhet i en rettsstat. Myndighetene har et ansvar for å utvikle slike tilstrekkelige rettssikkerhetsmekanismer, spesielt på et uavklart område som utfordrer personvernet.

Personvernkommisjonen mener bruk av maskinlæringssystemer i offentlig forvaltning bør forutsette menneskerettighetsvurderinger i tilfeller der systemene kan ha betydelig innvirkning på innbyggernes liv.

6.4.5 Profilering til kontrollformål

I mandatet til *Personvernkommisjonen* er det trukket frem at *kommisjonen* bør se nærmere på offentlig forvaltnings viderebehandling av personopplysninger til kontrollformål. Med utgangspunkt i mandatets ordlyd, fikk Mona Naomi Lintvedt i oppdrag fra *Personvernkommisjonen* å utarbeide en rapport med særlig vekt på bruk av profilering til kontrollformål i offentlig forvaltning.[69]

Personvernkommisjonen vil understreke at selv om mandatet vektlegger profilering til kontrollformål, betyr ikke dette at det ikke også er personvernutfordringer knyttet til bruk av profilering til andre formål. Profilering basert på maskinlæring anvendes også, som tidligere nevnt, til å målrette og tilpasse goder og tjenester til innbyggere. I tilfeller der maskinlæringssystemer brukes for å velge ut hvem som skal få og ikke få tilgang på goder fra det offentlige, kan det også oppstå problemer, for eksempel ved at individer feilaktig fratas goder de har krav på, eller at de ikke får tilstrekkelig informasjon.

---

[69] Lintvedt, M. N. (2022). *Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering*. Utredning for Personvernkommisjonen.

I rapporten skrevet på oppdrag fra *Personvernkommisjonen*, har Lintvedt blant annet vurdert et utvalg hjemler for innhenting og bruk av personopplysninger til kontrollformål i forvaltningen opp mot kravet om tydelig og presis lovhjemmel i personvernforordningen artikkel 6 nr. 3. Hun har også vurdert om bruk av profilering for utplukk til kontrollformål har rettsvirkning for den enkelte eller på tilsvarende måte i betydelig grad påvirker dem, jf. personvernforordningen artikkel 22 om automatiserte individuelle avgjørelser og profilering.

Lintvedt konkluderer blant annet med at lovhjemlene som gir behandlingsgrunnlag for Skatteetatens og NAVs innsamling av personopplysninger og bruk til profilering, bygger på utilstrekkelige vurderinger av forholdet til Grunnloven § 102 om respekt for privatliv, familieliv, sitt hjem og kommunikasjon. Det er heller ikke gjort tilstrekkelige vurderinger av artikkel 8 i Den europeiske menneskerettighetskonvensjonen (EMK) om respekt for privatliv og familieliv, og personvernhensyn i lys av personvernrettslige prinsipper. Lintvedt finner kun enkle, summariske vurderinger som grunnlag for hjemlene.

Lintvedt påpeker at Grunnloven, EMK og personopplysningsloven innebærer krav til utformingen av lovhjemler. Hvis lovhjemmelen er generelt utformet, er det viktig at vurderinger og nærmere avgrensninger er gjort i forarbeidene. Dessuten må mer detaljerte bestemmelser eventuelt følge av forskrift gitt med hjemmel i loven.

Personvernkommisjonen vil understreke at det er legitime grunner til å forhindre, kontrollere og avdekke misbruk av offentlige ordninger. I den sammenheng kan avanserte dataanalyser og profilering være hensiktsmessige og nødvendige virkemidler. Profilering behøver ikke medføre et stort inngrep. Profilering kan for eksempel anvendes for å forutsi noe om innbyggernes behov for informasjon og veiledning. Når risikovurderinger viser at anvendelser trolig har lite inngripende virkning og stor positiv effekt, vil etterlevelse av det alminnelige personvernregelverket være tilstrekkelig.

Personvernkommisjonen mener at profilering for å avdekke ulovligheter alltid bør sees som en inngripende behandling som krever solid hjemmel i lov, blant annet fordi det alltid er fare for utglidning fra beslutningsstøtte til beslutning (jf. eksempelet fra Nederland omtalt i avsnitt 6.2.5). Det må vurderes om inngrepet (her: profileringen) kan være lovlig etter EMK artikkel 8 andre ledd, herunder om det er «nødvendig 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 eller friheter». Inngrepet må være proporsjonalt i forhold til formålet som ønskes oppnådd og komme til utrykk i klare og forutsigbare rettsregler. Lovkravet innebærer at inngrepet må være hjemlet i nasjonal rett.

Det kan ikke overlates til etatene selv å utforme nærmere kriterier og retningslinjer for innsamling og bruk av personopplysninger for profileringsformål som har inngripende virkninger. At forvaltningen kan innhente nødvendige opplysninger om noe som kan være relevant for bredt formulerte formål, gir i denne sammenheng ikke tilstrekkelig rettsbeskyttelse og forutberegnelighet for innbyggerne.

Personvernkommisjonen mener offentlig forvaltning bør anvende føre-var-prinsippet ved bruk av profilering til kontrollformål. Utstrakt eller uforholdsmessig bruk av profilering til kontrollformål kan ha alvorlige negative effekter på individer og samfunnet, for eksempel i form av ulovlig forskjellsbehandling eller nedkjølingseffekter.

6.4.6 Offentlige aktører og store teknologiselskaper

Teknologimarkedet domineres av noen store selskaper, og flere av selskapene er tungt datadrevne. Dette kan utfordre personvernet. Utfordringene er likevel langt større enn bare hensynet til personvern. Forholdet til store teknologiselskaper berører mange andre rettsområder og demokratiske prinsipper.

I likhet med private aktører, benytter offentlige aktører tjenester fra de store teknologiselskapene. I flere sammenhenger kan dette være positivt. Selskapene leverer ofte tjenester av høy kvalitet og kan være et godt valg for å ivareta sikkerhet.[70] Videre kan det gjøre forvaltningen i stand til å møte innbyggerne på de digitale plattformene som innbyggerne benytter. Bruken av store teknologiselskaper medfører imidlertid klare utfordringer for personvernet. Personvernspørsmål og andre spørsmål knyttet til det offentliges bruk av tjenester fra store teknologiselskaper er mange og kompliserte. De er heller ikke begrenset til norsk forvaltning. På EU-nivå arbeides det aktivt med

[70] Det finnes ikke et entydig svar på om skytjenester gir god sikkerhet og dette beror på en sammensatt vurdering. Nasjonal Sikkerhetsmyndighet. (2022, 28. februar). *Samleside for skytjenester og sikkerhet*.

ulike tilnærminger til de store teknologiselskapene.[71]

I 2021 publiserte Datatilsynet sin interne personvernkonsekvensutredning av om tilsynet kunne være til stede på Facebook.[72] I den interne vurderingen ble det lagt til grunn at Datatilsynet ikke kan garantere for at innbyggernes personvern blir ivaretatt på Facebook, og at dette veide tyngre enn tilsynets behov for å kommunisere med innbyggere på plattformen.

Selv om vurderingen ikke er direkte overførbar eller bindende for andre offentlige organer, understreket tilsynet at bruken av gratis verktøy fra teknologigigantene betyr at offentlige virksomheter nærmest inviterer «kommersielle aktører til å samle inn og bruke data om norske innbyggere. Samtidig skapes det et avhengighetsforhold som det kan bli vanskelig å fri seg fra ettersom det finnes få alternative tjenestetilbydere».

I kjølvannet av publiseringen fulgte en rekke andre offentlige organer etter, inkludert Teknologirådet,[73] Bioteknologirådet, UDI og Sivilombudet,[74] ved å beslutte å avstå fra å bruke Facebook, mens andre, inkludert Politiet og Digitaliseringsdirektoratet, kom til motsatt konklusjon etter å ha gjort egne vurderinger. I sin interne personvernkonsekvensvurdering skriver Digitaliseringsdirektoratet blant annet at «det er liten risiko knyttet til behandlingens art, omfang, formål og sammenheng».[75] Vurderingen skiller seg markant fra vurderingene til Datatilsynet. Behovet for å nå ut til og å kommunisere med innbyggerne der de er tilstede ble vektlagt som viktige hensyn for både Politiet og Digitaliseringsdirektoratet.

Grunnen til at forskjellige offentlige aktører har endt opp med vidt forskjellige konklusjoner om bruk av Facebook, inkluderer ulike vurderinger av hvordan Facebook behandler personopplysninger, og om denne behandlingen innebærer risiko. Virksomheter vil også ha varierende behov for å nå ut til befolkningen for å utføre sitt samfunnsoppdrag, som vil påvirke interesseavveiingen. Bruken av sosiale medier bør også vurderes i lys av hvilke befolkningsgrupper virksomheten ønsker å nå ut til, og om dette kan oppnås på andre måter. Det må i alle tilfeller være en forutsetning at offentlige virksomheter har et bevisst forhold til eventuell bruk av sosiale medier, inkludert knyttet til personvernkonsekvenser ved deling av innhold.

Som beskrevet i kapittel 8, oppleves det uansett som lite hensiktsmessig at et stort antall mindre aktører, for eksempel i kommunesektoren, må gjøre helt egne vurderinger av avanserte plattformer og systemer, samt å utrede mulig personvernrisiko. For å sikre høy faglig kvalitet og god ressursbruk er det derfor viktig at forvaltningen samarbeider på tvers av sektorer ved gjennomføringen av nødvendige vurderinger. Dette vil også kunne lette byrden på de mindre aktørene i forvaltningen, som allerede opplever flere av vurderingene som svært krevende.

Personvernkommisjonen mener offentlige virksomheter må gjøre grundige vurderinger av om de skal benytte sosiale medier for å gi informasjon og kommunisere med innbyggerne. Sosiale medier bør ikke brukes i konkret enkeltsaksbehandling.

Personvernkommisjonen mener det er viktig at det gjøres både personvern- og datastrategiske vurderinger når det offentlige benytter tjenester fra store teknologiselskaper. Fordi spørsmålene ofte er likelydende, bør forvaltningen samarbeide på tvers av sektorer og nivåer for å sikre høy faglig kvalitet og god bruk av ressurser.

6.4.6.1 *Særskilt om sporing på offentlige nettsteder*

Som beskrevet i kapittel 9 om forbrukers personvern, eksisterer det et omfattende marked for innsamling, kjøp, salg og behandling av personopplysninger. Personopplysninger samles inn gjennom digitale tjenester og nettsider ved bruk av sporingsteknologi, som overfører informasjon om nettleserhistorikk, preferanser, demografisk informasjon og mye mer til et potensielt stort antall kommersielle tredjeparter

I 2021 gjennomførte Teknologirådet en undersøkelse av nettsidene til 41 aktører i offentlig sektor.[76] Undersøkelsen avdekket at 38 av aktørene anvendte sporingsteknologi fra kommersielle aktører på nettsidene. Det inkluderte deling av personopplysninger med en rekke tredjeparter, inkludert Facebook og Google. I noen tilfeller fant Teknologirådet sporingsteknologi som kan bru-

---

71 Det utarbeides blant annet regelverk, slik som Digital Markets Act, Digital Services Act og forordning for kunstig intelligens (AI Act). Disse beskrives nærmere i kapittel 9 om forbrukernes personvern.

72 Datatilsynet. (2021, 22. september). *Datatilsynet velger å ikke bruke Facebook*.

73 NRK. (2021, 6. oktober). *Teknologirådet mener mange offentlige aktører bør forlate Facebook*.

74 Sivilombudet. (2022, 13. juni). *Sivilombudet forlater Facebook og Instagram*.

75 Digitaliseringsdirektoratet. (u.å.). *Personvern på Facebook*.

76 Teknologirådet. (2021). *Kommersiell sporing i offentlig sektor*.

kes til å lage digitale fingeravtrykk eller ta opptak av brukerens aktiviteter på nettsider.

Teknologirådet beskriver det som et demokratisk problem at offentlige tjenester deler personopplysninger med kommersielle tredjeparter. Ifølge rådet er det som regel vanskelig eller umulig for innbyggerne å forstå hvordan sporingen fungerer, og datadelingen bidrar til å styrke teknologigigantenes monopoler. Innbyggerne har som regel ikke noe annet valg enn å besøke disse nettstedene, og kan dermed ikke velge bort sporingen. Derfor konkluderer Teknologirådet med at offentlige aktører bør avstå fra å bruke kommersiell sporingsteknologi. De anbefaler at offentlige aktører heller betaler for personvernvennlige løsninger for å gjennomføre analyser på sine nettsider.

Personvernkommisjonen støtter Teknologirådets betraktninger og anbefalinger. Offentlig sektor skal ikke betale for analyseverktøy og andre tjenester ved å utlevere innbyggernes personopplysninger, og har et særskilt ansvar for å fremme personvernvennlig teknologi.

Personvernkommisjonen mener offentlig forvaltning må tilgjengeliggjøre informasjon til innbyggerne i digitale løsninger der personopplysninger samles inn og brukes av kommersielle aktører til kommersielle formål, som for eksempel til å bygge og berike profiler eller deles med tredjeparter.

6.4.7 Informasjonssikkerhet

Informasjonssikkerhet blir et stadig større og viktigere område i takt med den økte digitaliseringen av samfunnet. Dette gjelder både for offentlige og private aktører.

Informasjonssikkerhet favner bredere enn personopplysningssikkerhet.[77] Informasjonssikkerhetsbrudd i løsninger som behandler personopplysninger, vil imidlertid ofte også medføre brudd på personopplysningssikkerheten. Tiltak som øker den generelle informasjonssikkerheten, vil derfor også kunne bidra til økt personopplysningssikkerhet. Dataangrepet mot Østre Toten i 2021 illustrerer dette, ved at mange av manglene knyttet til personopplysningssikkerhet i den saken også var generelle informasjonssikkerhetsmangler.

I januar 2021 ble Østre Toten kommune utsatt for et dataangrep. Angriperne fikk tilgang til kommunens datasystemer, krypterte all informasjon, og slettet sikkerhetskopiene.[78] Hendelsen resulterte blant annet i at kommunens systemer var utilgjengelige for ansatte, som førte til store kostnader og forsinkelser. I etterkant av hendelsen utstedte Datatilsynet et overtredelsesgebyr på fire millioner kroner til kommunen.[79] Ifølge tilsynet var det en rekke informasjonssikkerhetsmangler hos kommunen som muliggjorde hendelsen, inkludert fravær av gode sikkerhetsrutiner, logging av tilgang, samt mangel på tofaktorautorisering. Kommunen ble også pålagt å implementere et egnet styringssystem for informasjonssikkerhet og personopplysningssikkerhet.

Fra et overordnet perspektiv er det en utfordring for den generelle informasjonssikkerheten at virksomheter primært har fokus på, og vurderer, sikkerheten i egen virksomhet eller sektor. Dette kan medføre at mindre sårbarheter hos de enkelte virksomhetene samlet kan utgjøre større sårbarheter i et samfunnsperspektiv. På denne bakgrunn understreker *Personvernkommisjonen* viktigheten av det finnes offentlige nasjonale aktører som også vurderer informasjonssikkerheten samlet på et overordnet, nasjonalt nivå.[80]

Innbyggerne er avhengige av tjenester fra det offentlige. Innbyggere kan i liten grad påvirke om og hvordan personopplysningene behandles. For å ivareta evnen til å utføre oppgaver og tjenester, ivareta innbyggeres rettigheter og beholde den høye tilliten til offentlig forvaltning, er det særlig viktig å unngå brudd på informasjonssikkerheten i offentlige oppgaver og tjenester, inkludert digitale løsninger og infrastruktur. Viktigheten av god informasjonssikkerhet blir satt på spissen i store nasjonale IT-løsninger som behandler personopplysninger om alle innbyggere i Norge. Det er viktig med tilstrekkelige ressurser for å sikre et tilstrekkelig nivå på informasjonssikkerheten i slike løsninger.

Personvernkommisjonen mener virksomhetene i forvaltningen må få tydeligere anbefalinger (eller «norm») for styringsaktiviteter, og basisnivåer med sikkerhetstiltak og personverntiltak som de kan benytte som utgangspunkt ved styring av risiko for sine oppgaver og tjenester. Veiledning fra ulike myndigheter må henvise til hvilke deler av disse anbefalingene de veileder om, slik at det blir lett for virksomhetene og deres ledelse å benytte anbefalinger og veiledning til å ivareta sitt ansvar. Det må være en målsetning at dette skal gi

---

77 Se personvernforordningen art. 32.

78 NRK. (2021, 10. januar). *Sensitiv pasientinformasjon kan være på avveie etter dataangrep*.

79 Datatilsynet. (2022). *Overtredelsesgebyr til Østre Toten kommune*.

80 Digitaliseringsdirektoratet. (u.å.). *Nettverk for informasjonssikkerhet – NIFS*.

mer felles sikkerhet på tvers av forvaltningen, og et mer effektivt arbeid med informasjonssikkerhet og personvern i virksomhetene. Dette kan ivaretas gjennom tiltaket «Felles sikkerhet i forvaltningen». *Personvernkommisjonen* anbefaler at dette tiltaket gis prioritet som et sentralt finansiert tiltak og at statlige virksomheter med tilgrensende ansvarsområder gis oppdrag i tildelingsbrev med å bidra inn dette arbeidet.

6.5 Personvernkommisjonens anbefalinger oppsummert

Helhetlig tilnærming til personvern i offentlig forvaltning

- *Personvernkommisjonen* mener Stortinget bør sikres større innflytelse på digitaliseringen av offentlig forvaltning og hvilke konsekvenser dette får for innbyggernes personvern. Involvering av Stortinget bidrar blant annet til at beslutninger blir bedre belyst og får bredere forankring.
- *Personvernkommisjonen* mener tiltak med stor innvirkning på innbyggernes personvern bør hjemles i lov, i stedet for å forskriftsfestes. På den måten får Stortinget muligheten til å ha oversikt over forvaltningens behandling av personopplysninger.
- *Personvernkommisjonen* mener offentlige forvaltning har et særlig ansvar for å ivareta befolkningens tillit. Dette krever grundige vurderinger av om formålet med viderebehandlingen av innbyggernes personopplysninger er forenelig eller ikke med det opprinnelige innsamlingsformålet og hvor stort inngrep viderebehandlingen innebærer. Disse vurderingene bør offentliggjøres.
- *Personvernkommisjonen* anbefaler at regjeringen utarbeider en helhetlig personvernpolitikk for offentlig forvaltning. Personvernpolitikken må ses i sammenheng med digitaliseringspolitikken og gi føringer for hvordan forvaltningen skal gjøre prinsipielle vurderinger om personvern og sikre at borgernes personvern ivaretas i løsningene som utvikles. I personvernpolitikken bør regjeringen ha særlig oppmerksomhet på personvernkonsekvensene av mer utstrakt deling og viderebehandling av personopplysninger, og hvordan disse skal vurderes opp mot andre viktige hensyn som effektivisering og rettsikkerhet.
- *Personvernkommisjonen* anbefaler at regjeringen legger frem en personvernpolitisk redegjørelse for Stortinget årlig, forankret i gjeldende personvernpolitikk.
- *Personvernkommisjonen* mener det er et behov for et rådgivende og frittstående organ for forvaltningen som særlig skal vurdere og drøfte prinsipielle og generelle spørsmål knyttet til bruk av personopplysninger i offentlig forvaltning, herunder samfunnsmessige og etiske spørsmål.

Utforming av lovhjemler

- *Personvernkommisjonen* mener vurdering av personvernkonsekvenser i lovarbeid bør inkludere vurderinger av om eksisterende regelverk er tilstrekkelig og om det nasjonale handlingsrommet i personvernforordningen skal anvendes. Nasjonale bestemmelser kan gi klarere og mer utfyllende regler, og dermed større grad av forutberegnelighet for innbyggerne. Det vil også gi bedre grunnlag for å vurdere lovligheten av konkrete behandlinger av personopplysninger.
- *Personvernkommisjonen* anbefaler at regjeringen vurderer om rådføringsplikten etter personvernforordningen følges i tilstrekkelig grad. En slik vurdering bør også inneholde vurderinger av hvordan rådgivningsplikten kan innrettes for å ikke forsinke lovarbeidet samt føre til en uforholdsmessig stor ressursbelastning for Datatilsynet. Disse vurderingene bør gjøres som ledd i utviklingen av en personvernpolitikk.
- *Personvernkommisjonen* anbefaler at offentlig forvaltning offentliggjør vurderinger av personvernkonsekvenser i forbindelse med lov- og forskriftsarbeider.
- *Personvernkommisjonen* mener det er nødvendig å få på plass en forståelig og anvendelig veileder for vurdering av personvernkonsekvenser i lov- og forskriftsarbeid. Veilederen bør legge til rette for at ansvarlig departement kan synliggjøre både personvernkonsekvensene av det tiltaket som innføres isolert sett, og de samlede personvernkonsekvensene av ulike tiltak som allerede er på plass på det aktuelle området.
- *Personvernkommisjonen* mener veilederen om lovteknikk- og lovforberedelse («lovteknikkheftet») bør oppdateres.
- *Personvernkommisjonen* anbefaler at offentlig forvaltning styrker personvernkompetansen til ledere, saksbehandlere og andre ansatte som har behov for slik kompetanse. I arbeidet med regelverksutvikling bør det stilles krav til personvernkompetanse i arbeidsgruppen. Kunn-

skap om personvern bør inngå i den obligatoriske grunnopplæringen til nyansatte saksbehandlere, på lik linje med opplæring i forvaltningsloven og offentleglova.

Deling av personopplysninger mellom forvaltningsorganer

- *Personvernkommisjonen* anbefaler at ansvarsfordelingen i større grad lov- eller forskriftsfestes der deling av personopplysninger inngår som del av et større samarbeid mellom forvaltningsorganer og hvor uklarhet kan medføre alvorlige personvernkonsekvenser.
- *Personvernkommisjonen* mener det må utarbeides og videreutvikles standarder for deling av personopplysninger. Dette gjør det lettere å samarbeide, og bidrar til å sikre høyere faglig kvalitet og effektiv ressursbruk.
- *Personvernkommisjonen* anbefaler at regjeringen utreder om en samtykkebasert gjennomføring av «kun-en-gang'-prinsippet vil kunne avhjelpe noen av personvernulempene som oppstår ved deling av personopplysningen mellom offentlige etater.
- *Personvernkommisjonen* anbefaler at Kommunal- og distriktsdepartementet følger opp rapporten til Digdir om innsyn og kontroll med hvordan personopplysninger behandles i offentlige virksomheter i arbeidet med å tilrettelegge for god ivaretakelse av innbyggernes rettigheter i offentlig forvaltning.

Bruk av kunstig intelligens

- *Personvernkommisjonen* mener lovregulering av bruk av kunstig intelligens bør ha som formål å motvirke maktubalansen mellom offentlig forvaltning og innbyggerne. Jo mer inngripende, dess større krav bør en stille til åpenhet og andre rettsikkerhetsmekanismer.
- *Personvernkommisjonen* mener bruk av maskinlæringssystemer i offentlig forvaltning bør forutsette menneskerettighetsvurderinger i tilfeller der systemene kan ha betydelig innvirkning på innbyggernes liv.

Profilering til kontrollformål

- *Personvernkommisjonen* mener at profilering for å avdekke ulovligheter alltid bør sees som en inngripende behandling som krever solid hjemmel i lov, blant annet fordi det alltid er fare for utglidning fra beslutningsstøtte til beslutning. Inngrepet må være proporsjonalt i forhold til formålet som ønskes oppnådd og komme til utrykk i klare og forutsigbare rettsregler.
- *Personvernkommisjonen* mener offentlig forvaltning bør anvende føre-var-prinsippet ved bruk av profilering til kontrollformål. Utstrakt eller uforholdsmessig bruk av profilering til kontrollformål kan ha alvorlige negative effekter på individer og samfunnet.

Offentlige aktører og store teknologiselskaper

- *Personvernkommisjonen* mener offentlige virksomheter må gjøre grundige vurderinger av om de skal benytte sosiale medier for å gi informasjon og kommunisere med innbyggerne. Sosiale medier bør ikke brukes i konkret enkeltsaksbehandling.
- *Personvernkommisjonen* mener det er viktig at det gjøres både personvern- og datastrategiske vurderinger når det offentlige benytter tjenester fra store teknologiselskaper. Fordi spørsmålene ofte er likelydende, bør forvaltningen samarbeide på tvers av sektorer og nivåer for å sikre høy faglig kvalitet og god bruk av ressurser.
- *Personvernkommisjonen* mener offentlig forvaltning må tilgjengeliggjøre informasjon til innbyggerne i digitale løsninger der personopplysninger samles inn og brukes av kommersielle aktører til kommersielle formål, som for eksempel til å bygge og berike profiler eller deles med tredjeparter.

Informasjonssikkerhet

- *Personvernkommisjonen* mener virksomhetene i forvaltningen må få tydeligere anbefalinger (eller «norm») for styringsaktiviteter, og basisnivåer med sikkerhetstiltak og personverntiltak som de kan benytte som utgangspunkt ved styring av risiko for sine oppgaver og tjenester.
- *Personvernkommisjonen* anbefaler at regjeringen gir tiltaket «Felles sikkerhet i forvaltningen» prioritet som et sentralt finansiert tiltak. Statlige virksomheter med tilgrensende ansvarsområder gis oppdrag i tildelingsbrev om å bidra inn i dette arbeidet.

Kapittel 7
Personvern i justissektoren

7.1 Innledning

Personvernkommisjonen skal i følge mandatet «se på utviklingen av personvern i justissektoren og identifisere i hvilken grad det samlede omfanget av tiltak skaper utfordringer for personvernet». Dette er en svært vid oppgave, som utvilsomt kunne vært tema for en egen spesifikk utredning. Mandatspørsmålets ordlyd reiser flere spørsmål, til dels av prinsipiell karakter.

I en demokratisk rettsstat må enkeltpersoners rett til selvbestemmelse og frihet balanseres med myndighetenes muligheter til å gripe inn mot individet. Dette kommer ikke minst til syne i justissektoren, hvor kriminalitetsbekjempelse og personvern vil kunne komme i konflikt. Endringer i kriminalitetsbildet, blant annet som en følge av digitaliseringen, gjør at justissektoren har behov for og ønsker å ta i bruk nye verktøy og metoder som til dels kan være svært inngripende. Utviklingen bidrar også til at både strafferettslige og metodemessige lovendringer iverksettes for å kunne håndtere nye utfordringer.

Digitaliseringen fører til at eksisterende tiltak kan bli mer inngripende. Mens etterforskningsmetoder tidligere kunne være begrenset til fysiske inngrep, er det i dag mulig å innhente store mengder informasjon om hele befolkningen ved hjelp av digitale verktøy. Som beskrevet i kapittel 9, blir store mengder informasjon om hver enkelt av oss automatisk registrert gjennom forskjellige sporingsteknologier, blant annet når vi bruker sosiale medier, kommuniserer digitalt, og når vi beveger oss rundt med mobiltelefonen i lommen. Dersom grunnleggende personvernprinsipper ikke ivaretas i tilstrekkelig grad, kan dette bidra til at man går fra målrettede inngrep mot enkeltindivider eller grupper, til at informasjon om store grupper innhentes og analyseres i forsøk på å avdekke kriminalitet. Det er nødvendig med robuste forutgående vurderinger og etterfølgende kontrollmekanismer som sørger for at inngrep i personvernet ikke blir for vidtgående, er proporsjonale og i tråd med lov og forskrift.

Ved bruk av inngripende metoder i justissektoren vil det i mange tilfeller være snakk om å bekjempe alvorlig kriminalitet, inkludert terror, vold, drap og seksuelle overgrep. Dette er formål som gjør at inngrep ofte vil regnes som nødvendige og viktige. Selv om bekjempelse og forebygging av alvorlig kriminalitet utvilsomt er nødvendig, er det en forutsetning at grunnleggende personvernprinsipper ligger til grunn for å sikre forutberegnelighet og rettferdig behandling av personopplysninger. Dette gjelder både for involverte parter i en kriminalsak og for befolkningen som helhet.

De fleste innbyggere har lite kontakt med justissektoren i det daglige. I mange tilfeller vil det være særlig sårbare eller utsatte individer og grupper som er i kontakt med sektoren. Dersom det er snakk om personer som har begrenset evne eller mulighet til å kjenne og ivareta sine personvernrettigheter, er det grunn til å utvise særlig aktsomhet.

I dette kapitlet vil *Personvernkommisjonen* søke å beskrive spenningen som kan oppstå mellom kriminalitetsbekjempelse og innbyggernes personvern. Disse spørsmålene henger uløselig sammen med forholdet mellom sikkerhet og frihet i et demokratisk samfunn. Forutsetningen må være at kriminalitetsbekjempelse og forebygging skjer på en ansvarlig måte. Retten til privatliv og tilhørende personvern skal stå sentralt i et moderne demokrati. På den annen side skal kriminalitet bekjempes og forebygges. Det er i det spenningsforholdet som kan oppstå her at *kommisjonen* gjør sine vurderinger.

7.1.1 Definisjoner, avgrensninger og metodologiske utfordringer

Hvilke institusjoner eller oppgaver som hører inn under «justissektoren» vil avhenge av konteksten. I følge Justis- og beredskapsdepartementet finnes

det ikke en offisiell definisjon av hvilke institusjoner som hører inn under begrepet.

Politiet, herunder Politiets sikkerhetstjeneste (PST), kriminalomsorgen, påtalemyndigheten og domstolene hører naturlig til justissektor-begrepet. Det samme gjelder Statens sivilrettsforvaltning, Sysselmesteren på Svalbard, Kontoret for voldsoffererstatning, Tilsynsrådet for advokatvirksomhet og Kommisjonen for gjenopptakelse av straffesaker. Den militære etterretningstjenesten er en del av forsvarssektoren og vil dermed ikke bli behandlet direkte i denne rapporten.

Sektorer som vekterbransjen og Tolletaten har enkelte ansvarsområder og arbeidsoppgaver som kan ligne på de som utføres av virksomheter i justissektoren. *Kommisjonen* avgrenser imidlertid rapporten mot disse, og behandling av personopplysninger og eksempler fra disse områdene benyttes kun der de belyser situasjonen.

Hoveddrøftelsen i kapitlet knyttes til politiet. *Kommisjonen* har i begrenset grad hatt kapasitet og ressurser til å vurdere de øvrige myndighetsområdene nevnt over og særskilte problemstillinger som kan reises der. Viktigere ved denne avgrensning er at politiet og dets arbeid i særlig grad er illustrerende for de kryssende hensyn som foreligger og den nødvendige vektingen av personvern som alltid må foretas. Med Politiets sikkerhetstjenestes (PST) ansvar for bekjempelse av terror oppstår helt spesielle problemstillinger, ikke minst knyttet til den foreliggende terrortrussel, hvor reell er denne og hvilke tiltak en adekvat bekjempelse fordrer.

Med den tid som sto til disposisjon for *kommisjonens* arbeid har det ikke vært mulig å gå inn i alle ulike spørsmål knyttet til spesifikke politioppgaver. *Personvernkommisjonen* har måttet nøye seg med de generelle spørsmål på et aggregert nivå. Det tillegges at som kjent fører Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget) løpende kontroll med PSTs arbeid. Denne kontrollen innbefatter også personopplysningsloven og kontroll av informasjon og behandling av personopplysninger.

Personvernkommisjonen benytter ved flere anledninger begrepet kriminalitetsbekjempelse. I denne sammenheng omfatter begrepet alle aspekter ved kriminalitetsbekjempelse som eksempelvis; forebyggende arbeid, politietterforskning, iretteføring for domstolene, domfellelse og oppfølging i regi av kriminalomsorgen. De ulike aktivitetene har som hovedformål å bekjempe kriminalitet. *Kommisjonen* har i noe mer begrenset omfang enn forventet fått tilgang til informasjon om hvordan prosedyrer og rutiner for behandling av personopplysninger faktisk praktiseres i de ulike politidistrikt i Norge. Det har også vært utfordringer knyttet til å få innsikt i metodebruk og verktøy som er i bruk eller som vurderes tatt i bruk. Det faktum at det har vært utfordrende å få tilgang til relevante opplysninger, er interessant i seg selv. *Kommisjonen* ser det som problematisk at det er begrenset offentlig informasjon tilgjengelig om hvilke verktøy politiet anvender i dag eller vurderer å anvende i fremtiden. Dette gjør det vanskelig å bedømme eventuelle personvernkonsekvenser ved metodebruken.

Kommisjonen har også drøftet hvorvidt en kartlegging av ulike tiltak og deres samlede effekt for personvernet har gyldighet over tid. Politiet forventes å være tilpasningsdyktig og igangsette egnede tiltak som svarer på risikobildet i samfunnet slik det til enhver tid foreligger. Vurderinger som kun bygger på et statisk bilde av politiets tiltak i dag, vil fort bli utdatert og dermed miste nytteverdi.

På denne bakgrunn søker *kommisjonen* å besvare mandatet ved å drøfte rammebetingelsene for at tiltak som politiet kan benytte er i tråd med godt personvern, istedenfor å utrede ulike tiltak hver for seg.

Følgende prinsipielle rammebetingelser vil drøftes;

- Rettslig regulering.
- Grundige vurderinger av personvernkonsekvenser og interesseavveining mot andre samfunnsinteresser.
- Åpenhet om ulike tiltak som politiet har til rådighet.
- Reell internkontroll.
- Effektiv domstolskontroll.
- Reell mulighet til å håndheve personvernrettigheter.
- Adekvat tilsyn og håndheving av regelverket.

Disse prinsipielle rammebetingelsene er avgjørende for reell ivaretakelse av personvernet. Dersom de ikke foreligger er det etter *kommisjonens* syn nærliggende å anta at personvernet ikke i tilstrekkelig grad kan ivaretas.

7.1.2 Personvern i justissektoren – en rettssikkerhetsgaranti

I den offentlige debatten betones det ofte at det er et grunnleggende spenningsforhold mellom godt personvern og effektiv kriminalitetsbekjempelse, noe som kan føre til ulike former for konflikt. Etter *kommisjonens* oppfatning er en slik tilnær-

ming for snever. I flere sammenhenger vil en tilstrekkelig kriminalitetsbekjempelse utvilsomt være en forutsetning for godt personvern, ikke minst gjennom oppklaring og iretteføring for domstolene. I mange tilfeller vil også godt personvern kunne bidra til forebygging av kriminalitet, for eksempel ved at kriminelle aktører har mindre tilgang på opplysninger som kan misbrukes til svindel og identitetstyveri.

En nødvendig forutsetning for god kriminalitetsbekjempelse er at grunnleggende interesser balanseres. Ved oppklaring av all alvorlig kriminalitet er det et gjennomgående trekk at viktige hensyn ofte trekker i ulike retninger. Mistenktes interesser kontra hensynene til offeret er et eksempel på dette. Tilsvarende gjelder effektivitet og rettssikkerhet. Det er ingen tvil om at man med enkle grep kan gjøre inngripende tiltak langt mer effektive. I et demokratisk samfunn er begrensningen av slike tiltak likevel nødvendig selv om det i noen tilfeller kan føre til mindre effektiv kriminalitetsbekjempelse. Samfunnet må som sådan ta konsekvensene av å ikke ta i bruk alle tilgjengelige virkemidler for å bekjempe kriminalitet. Det samme vil gjelde dersom virkningene av inngripende tiltak blir for vidtgående.

I en god rettsstat må verdier og kryssende hensyn veies mot hverandre. Hvordan og hvor grundig man utfører en slik interesseavveining, på både systemnivå og i hver enkelt sak, sier noe om rettsstatens kvalitet. I merknadene til politiregisterloven § 1 (lovens formål) heter det: «I de tilfellene der hensynet til personvern og hensynet til kriminalitetsbekjempelsen ikke kan forenes, er *utgangspunktet at hensynet til personvernet må vike*.» Denne betraktningen, om at bekjempelse av kriminalitet har forrang ved en konflikt med personvernet – selv om det i forarbeidene gis anvisning på en forholdsmessighetsvurdering – er *kommisjonen* ikke enig i. Hvordan ulike interesser vektes, vil være avgjørende for hvilken løsning som velges. Når interesser står mot hverandre, kan ikke utgangspunktet være at personvernet alltid må vike.

Dersom personvernkrenkelsen som følge av et tiltak er tilstrekkelig alvorlig, må konklusjonen etter *Personvernkommisjonens* oppfatning være den motsatte; kriminalitetsbekjempelsen skal vike.

7.1.3 Viktigheten av tillit til justissektoren

Tillit er en grunnleggende forutsetning for et fungerende demokrati, og er, som nevnt, nødvendig for at justissektoren skal kunne gjennomføre sine oppgaver. For å ivareta tilliten i befolkningen må sektoren være i stand til å bekjempe og forebygge kriminalitet.

Tillit til justissektoren er også avhengig av at befolkningen har innsikt i hvordan deres grunnleggende rettigheter ivaretas. Dette forutsetter en viss grad av informasjon og åpenhet, både om vurderingene som gjøres og om metodene som benyttes. Det kan imidlertid være utfordrende for justissektoren å utvise åpenhet om vurderinger og metodebruk i konkrete saker. Dersom beskrivelsen av vurderingene som gjøres og metodene som benyttes blir for detaljert, vil dette kunne gjøre effektiv kriminalitetsbekjempelse mer utfordrende. Vidtgående kontrollregimer, uten at det balanseres med en viss grad av åpenhet og rettssikkerhetsgarantier, vil imidlertid over tid utfordre innbyggernes tillit til justissektoren.

Dersom tilliten ikke er til stede, kan det få praktisk betydning for kriminalitetsbekjempelsen. Miljøer eller individer som urettmessig stadig utsettes for undersøkelser og kontroll basert på vidtgående inngrepshjemler, vil ikke ønske å gi informasjon til personell de kontrolleres av. Undersøkelser og kontroll igangsatt av etater man har tillit til, vil derimot oppleves annerledes. En kriminalitetsbekjempende organisasjon som forvalter og ivaretar grunnleggende menneskerettigheter, vil enklere få tilgang til nødvendige opplysninger.

Boks 7.1 Tillit til justissektoren

Det er generelt høy tillit til justissektoren i Norge. I følge Tiltro-undersøkelsen er tilliten til domstolene svært høy, og hele 92 prosent av befolkningen hadde svært eller ganske stor tiltro til domstolene i 2020.[1] Det fremkommer av Datatilsynets personvernundersøkelse at innbyggernes tillit til politiet også er høy, da nær fire av fem har ganske stor eller svært stor tillit. Politiets innbyggerundersøkelse for 2020 viser at 82 prosent av de spurte svarer at de har tillit til politiet.

[1] Rett24. (2021, 5. januar). *Tiltroen til myndighetene rett til værs i korona-Norge.*

7.2 Rettslig regulering av personvern i justissektoren

Det sentrale personvernregelverket for politi og påtalemyndighet er politiregisterloven med tilhørende politiregisterforskrift[1] og personopplysningsloven. Politi og påtalemyndighet må derfor forholde seg til to regelsett som direkte regulerer behandling av personopplysninger, i tillegg til en rekke andre lovverk. De senere år er det blitt gjennomført en rekke lovendringer som skal tilrettelegge for kriminalitetsbekjempelse i det digitale samfunnet. Dette stiller krav til kompetanse og krever at sektoren er oppdatert på regelverket. I det følgende vil *Personvernkommisjonen* se nærmere på de mest sentrale regelverkene for sektorens behandling av personopplysninger. Rettighetene i EMK artikkel 8 og adgangen til å gjøre inngrep i disse, vil omtales kort. *Kommisjonen* behandler i tillegg domstolskontroll med politiets tiltak. I tillegg vil *kommisjonen* gi en kort oversikt over hvordan personopplysninger behandles i politiet, domstolene og kriminalomsorgen.

7.2.1 Kort om artikkel 8 i EMK og adgangen til å gjøre inngrep

EMK artikkel 8 oppstiller et generelt vern om privat- og familieliv, hjem og korrespondanse. Retten til privatliv er imidlertid ikke absolutt, siden begrepet «respect» gir anvisning på at privatlivet skal respekteres, ikke at det foreligger et totalforbud mot inngrep i denne rettigheten, jf. EMK artikkel 8 nr. 1. Inngrep i rettighetene som er nedfelt i første ledd kan være lovlige dersom de er «nødvendig av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forbygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter eller friheter» jf. EMK artikkel 8 nr. 2.

Menneskerettsdomstolen (EMD) har omfattende praksis for tolkning av disse kriteriene. Det må vurderes om tiltaket som griper inn i personvernet er forsvarlig og nødvendig i et demokratisk samfunn. Inngrepet må dessuten være proporsjonalt i forhold til formålet som ønskes oppnådd, og komme til utrykk i klare og forutsigbare rettsregler. Lovkravet innebærer at inngrepet må være hjemlet i nasjonal rett.[2]

Når EMD vurderer hvorvidt staten kan holdes ansvarlig for en krenkelse av EMK artikkel 8, er det flere forhold som spiller inn. Først må det bringes på det rene hvorvidt forholdet angår noens privatliv. Videre vil domstolen undersøke hvorvidt fakta i saken indikerer at det har skjedd et inngrep i retten til privatliv. Domstolen har gjennom sin praksis trukket frem mange ulike forhold som griper inn i retten til privatliv: familievold som truer kroppslig integritet,[3] forhold knyttet til seksuelle og reproduktive rettigheter,[4] medisinsk behandling uten samtykke,[5] og til og med forhold knyttet til forurensning og retten til et ikke-helseskadelig miljø[6] såfremt de innvirker på ens helse eller livskvalitet.[7]

Når det gjelder retten til personvern ved behandling av personopplysninger, har ulike forhold knyttet til innhenting av personopplysninger,[8] lagring av opplysninger,[9] tilgjengeliggjøring eller utlevering[10] blitt vurdert som inngripende i retten til privatliv. På samme måte, har domstolen behandlet saker der en person er blitt nektet tilgang til personopplysninger, eller ikke har fått mulighet til å korrigere eller slette personopplysninger, og har drøftet hvorvidt slike begrensninger kan rettferdiggjøres eller ikke.

Selv om slike ovennevnte forhold griper inn i noens private sfære, betyr ikke det automatisk at domstolen oppfatter disse som krenkelser av pri-

---

1 Forskrift 20. september 2013 nr. 1097 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterforskriften).

2 *Sunday Times v. The United Kingdom*, [J], no. 6538/74, (1980), Series A no 38, avsnitt 47.

3 *Milićević v. Montenegro*, [J], no. 27821/16, (2018) ECHR:2018:1106, § 54-56.
E.S. and Others v. Slovakia, [J] no. 8227/04, (2009), ECHR:2009:0915, § 44.

4 *Ternovszky v. Hungary*, [J] no. 67545/09, (2010), ECHR:2010:1214 § 22, *S.H. and Others v. Austria* [GC], no. 57813/00, (2011), ECHR:2011:1103. § 82; *Knecht v. Romania*, [J] no. 10048/10, (2012), ECHR:2012:1002, § 54.

5 *Glass v. the United Kingdom*, [J], no. 61827/00, (2004), ECHR:2004:0309.
Jalloh v. Germany [GC], no. 54810/00, (2006), ECHR:2006:0711, § 70.
Schmidt v. Germany, [J], no. 13580/88, (1994), ECHR:1994:0718.

6 *Çiçek and Others v. Turkey* (dec.), [J] nos. 74069/01, 74703/01, 76380/01, 16809/02, 25710/02, 25714/02 and 30383/02, (2007), ECHR:2007:0503 § 32 and §§ 22-29.

7 *Fadeyeva v. Russia*, [J], no. 55723/00, (2005), ECHR:2005:0609, § 68-69.

8 European Court of Human Rights. (2021). *Guide to the Case-Law of the European Court of Human Rights: Data Protection*. Avsnitt 122-192.

9 European Court of Human Rights. (2021). *Guide to the Case-Law of the European Court of Human Rights: Data Protection,* avsnitt 192-227.

10 European Court of Human Rights. (2021). *Guide to the Case-Law of the European Court of Human Rights: Data Protection*, avsnitt 228-261.

vatlivet, det vil si som ulovlige inngrep. Det foretas en grundig vurdering for å konkludere om dette.

Det tredje og utslagsgivende steget i domstolens vurdering, er hvorvidt inngrepet er «akseptabelt» etter kravene i 2. ledd, det vil si hvorvidt de er i samsvar med loven, er nødvendige og forholdsmessige.

Når det gjelder politiets bruk av tvangsmidler, må det foretas en konkret vurdering av blant annet inngrepets varighet og intensitet, hvilken mistankegrad som foreligger, om overvåkningen fant sted åpent eller skjult, om informasjonsinnhentingen skjedde systematisk og permanent, og på hvilken måte beslutningen om overvåkning ble fattet. Helhetsvurderingen rommer på dette grunnlag viktige personvern- og rettsikkerhetsvurderinger. For at tvangsmiddelbruk ikke skal innebære en krenkelse av privatlivet, må inngrepet oppfylle vilkårene i EMK artikkel 8 nr. 2.

7.2.2 Politiregisterloven

Politiet behandler personopplysninger etter flere regelverk, avhengig av hva som er formålet med behandlingen. I det følgende vil *kommisjonen* kort redegjøre for politiregisterlovens bestemmelser for behandling av personopplysninger i politiet.

Politiregisterloven har som formål å «bidra til effektiv løsning av politiets og påtalemyndighetens oppgaver, beskyttelse av personvernet og forutberegnelighet for den enkelte ved behandlingen av opplysninger».[11] Loven regulerer blant annet behandling av personopplysninger i politiets 19 registre. Politiregistrene inkluderer blant annet DNA-registeret, fingeravtrykkregisteret, fotoregisteret, straffesakregisteret, utlendingsregisteret, personidentitetsregistret og hvitvaskingsregisteret.

Kripos har behandlingsansvar for 17 registre, mens Politiets utlendingsenhet og Økokrim har ansvar for ett register hver. Den behandlingsansvarlige enheten skal sørge for at behandlingen skjer i henhold til reglene for blant annet informasjonssikkerhet, internkontroll og bruken av registrene.

Politidirektivet, politiregisterloven og tilhørende forskrift stiller ulike krav til om personopplysninger kan behandles, hvordan slike opplysninger skal behandles og hvilke vurderinger politiet skal gjøre for å ivareta personvernet. Hjemlene åpner for at politiet kan utøve skjønn med tanke på hvorvidt hjemlene kan tas i bruk i en konkret sak og hvilke rettsikkerhetsgarantier som skal iverksettes.

Det er Datatilsynets ansvar å føre tilsyn med behandlingen av personopplysninger i politiet og påtalemyndigheten.[12] Unntakene er opplysninger som behandles av Politiets sikkerhetstjeneste (PST), og politiets behandling av saker om kommunikasjonskontroll.[13] Se nærmere omtale av Datatilsynets tilsynskompetanse i kapittel 13.

Politiregisterloven inneholder egne bestemmelser om behandling av personopplysninger i PST. Generelt kan det sies at PST har et større spillerom ved behandling av personopplysninger enn det ordinære politiet har. PST er i tillegg unntatt fra Datatilsynets tilsynskompetanse. Kompetanse til å føre tilsyn med PSTs behandling av personopplysninger ligger i stedet hos Stortingets eget kontrollutvalg for de hemmelige tjenestene (EOS-utvalget).

Behandlingsansvaret for politiets behandling av personopplysninger er fordelt på ulike instanser avhengig av formålet med behandlingen. Kripos er, som tidligere nevnt, behandlingsansvarlig for 17 av de totalt 19 sentrale registrene, et ansvar de er tildelt gjennom forskrift.[14] De ulike politidistriktene er imidlertid behandlingsansvarlig for personopplysninger knyttet til straffesaker som behandles ved de respektive distriktene.[15] Personopplysninger som behandles i politiets forvaltningsvirksomhet og for sivile gjøremål, og som faller under personvernforordningens virkeområde, er under Politidirektoratets behandlingsansvar. Kripos er behandlingsansvarlig for personopplysninger som blir behandlet etter lov om Schengen informasjonssystem (SIS).[16] PST er selv behandlingsansvarlig for behandling av personopplysninger i forbindelse med tjenestens arbeid, herunder å forebygge straffbare forhold, utarbeidelse av trusselvurderinger og samarbeid med andre lands politi- og sikkerhetsmyndigheter.[17]

Det følger av politiregisterloven § 63 at det skal etableres en ordning med *personvernrådgiver.*

---

11 Politiregisterloven § 1.

12 Se politiregisterloven § 58 og politiregisterforskriften § 42-1.

13 Datatilsynet. (2018). *Om politiregisterloven*.

14 Se politiregisterforskriften § 44-3.

15 Politiregisterforskriften § 2-1.

16 Informasjonssystemet i Schengen (og andre generasjon av systemet – SIS II) er en av hjørnestenene i Schengen-samarbeidet. Det er et informasjonssystem som gjør at de nasjonale grense-, toll- og politimyndighetene som er ansvarlige for kontroller ved Schengen-områdets eksterne grenser så vel som innenfor Schengen-området, kan dele varsler om etterlyste eller savnede personer samt objekter som stjålne kjøretøyer og dokumenter.

17 Se politiregisterforskriften § 20-4 jf. § 20-2.

Betegnelsen personvernrådgiver ble benyttet fordi begrepet personvernombud, i følge justisdepartementet, ville «by på utfordringer i forholdet mellom rollebetegnelse og rollekompetanse».[18]

Personvernrådgiverens oppgaver samsvarer i stor grad med et personvernombuds oppgaver etter personvernforordningen.[19] I følge politiregisterforskriften skal personvernrådgiveren påse at det finnes systemer for internkontroll, påpeke brudd, gi råd og veiledning og bistå de registrerte. Det kan se ut som om personvernrådgiveren ikke skal ha samme kontrollfunksjon som personvernombudet har etter personvernforordningen.[20] Av forarbeidene fremgår at personvernrådgiverens rolle skal «være både rådgivende og kontrollerende i forhold til den behandlingsansvarlige og den enkelte som behandler opplysningene».[21]

Oslo politidistrikt, Kripos, Politihøgskolen og Økokrim har egne personvernombud etter personopplysningsloven. I tillegg til dette har alle andre enheter i politiet et felles personvernombud i Politidirektoratet. Dette personvernombudet skal ha en kontaktperson for personvern i alle de øvrige politidistriktene og særorganene.[22] I tillegg til dette finnes det personvernrådgivere i hvert distrikt.

Personvernrådgiverne i politiet behandler saker som gjelder personvern i de enkelte politidistriktene. Personvernrådgiverne bidrar også med innspill om ivaretakelse av personvernet ved utvikling av nye politimetoder, og i arbeid på strategisk nivå der personvernspørsmål er relevant.

7.2.2.1 Forholdet mellom politiregisterloven og personopplysningsloven

Etter personvernforordningen skal personopplysninger behandles for uttrykkelige angitte formål og ikke viderebehandles for formål som ikke er forenlige med det opprinnelige formål.[23] Politiregisterloven er basert på samme prinsipper og fastslår at opplysninger bare kan behandles dersom dette er nødvendig og relevant for nærmere angitte formål, jf. politiregisterloven §§ 4 og 5. Etter politiregisterloven § 4 kan imidlertid personopplysninger også behandles for «*andre politimessige formål*», i tillegg til det opprinnelige formålet med innhentingen.[24] Politimessige formål omfatter politiets kriminalitetsbekjempende virksomhet, herunder etterforskning, forebyggende arbeid og ordenstjeneste, politiets service- og bistandsfunksjon, samt føring av vaktjournaler.[25]

Bestemmelsen i politiregisterloven § 4 gir uttrykk for at opplysningene som hovedregel kan brukes fritt innenfor de ulike politimessige formålene. Dette innebærer for eksempel at opplysninger innhentet i forbindelse med etterforskning kan brukes til politiets bistands- og servicefunksjon og vice versa.

Tilgang til opplysninger i politiet gis til tjenestepersoner i politiet og påtalemyndigheten med et «tjenestemessig behov» for tilgang, og til formål som omfattes av politiregisterloven, jf. politiregisterloven § 21 jf. politiregisterforskriften § 8-3. Vilkåret «tjenestemessig behov» vil være oppfylt dersom tjenestemannen vil settes i stand til å treffe en riktigere eller mer begrunnet avgjørelse, eller utføre en mer effektiv og hensiktsmessig tjeneste, enn om vedkommende ikke hadde hatt tilgang til opplysningene, jf. politiregisterforskriften § 8-3 annet ledd. Dette innebærer at politiet har et betydelig rom for å benytte opplysninger som er innhentet i forbindelse med for eksempel servicefunksjonen i en senere etterforskning, dersom dette anses som nødvendig.[26] Til tross for at bestemmelsene som omhandler tjenestemessig behov har rom for skjønnsmessige vurderinger, danner prinsippene om formålsbestemthet og nødvendighet rammene for hvilken bruk som faller innenfor regelverkets rammer.

Beslutningskompetansen til å utlevere opplysninger følger av politiregisterforskriften § 11-2. For registrene Kripos er behandlingsansvarlig for er adgangen i mange tilfeller delegert ut til enhetene i politiet, som igjen kan delegere ned til tjenestepersonnivå i lokale rutiner. Politiregisterforskriften § 11-2 siste ledd definerer i hvilke tilfeller den enkelte tjenestemann alltid kan beslutte utlevering eller bruk av opplysninger. Det er Politidirektoratet eller riksadvokaten som beslutter eventuell utlevering av opplysninger til forskning, jf. politiregisterloven § 33 annet ledd jf. politiregisterforskriften § 11-2 annet ledd.

---

18 Se Ot.prp. nr. 108 (2008–2009) side 268.

19 Se politiregisterforskriften § 43-1 og personvernforordningen artikkel 39.

20 Se personvernforordningen art. 39 bokstav b.

21 Se Ot.prp. nr. 108 (2008–2009) side 325.

22 Politiet. (u.å.). *Politiets Personvernerklæring*.

23 Personvernforordningen art. 6 bokstav b.

24 Politiregisterloven § 4.

25 Se politiregisterloven § 2 (13).

26 I politiregisterlovens forarbeider fremkommer det at man har valgt å videreføre en vid definisjon av tjenestemessig behov, da man ikke vil at loven skal være et hinder for at tjenestepersoner og ansatte i etaten kan utføre sitt kriminalitetsbekjempende arbeid. Se NOU 2003: 21 *Kriminalitetsbekjempelse og personvern – Politiets og påtalemyndighetens behandling av opplysninger*.

Behandling av personopplysninger i etterforskningssammenheng[27] reguleres også av straffeprosessloven. Det er flere bestemmelser i straffeprosessloven som omhandler innhenting, håndtering og utlevering av personopplysninger. Slik virksomhet faller utenfor personvernforordningens materielle virkeområde.[28] Behandling av personopplysninger med grunnlag i politiets forvaltningsvirksomhet og sivile gjøremål omfattes av personopplysningsloven og personvernforordningen.[29]

7.2.3 Domstolskontroll

I *Personvernkommisjonens* vurderinger av i hvilken grad det samlede omfang av tiltak innenfor sektoren skaper særskilte utfordringer for personvernet, må rettssikkerhetsmekanismene som ligger innebygd i lovverket berøres kort. Dette gjelder særlig domstolskontroll.

Alle tvangsmidler krever hjemmel i lov. Legalitetsprinsippet som følger av Grunnloven[30] inneholder et klarhetskrav for å kunne anvende straff (ordlyden må være presis) og et analogiforbud (loven kan ikke anvendes på tilfeller som ikke omfattes). Når det gjelder beslutningskompetanse, er det nærmere regulert i lov om kompetansen ligger til polititjenestemenn, påtalemyndigheten i politiet eller domstolene, og for hvilke tvangsmidler, og i hvilke situasjoner kompetansen skal gjelde. Jo mer inngripende et tiltak er, desto strengere er kravene til kontroll før tiltaket iverksettes.

Politiets fullmakter er utvilsomt utvidet de senere år, ikke minst i sammenheng med frykten for alvorlige terrorangrep, også på norsk jord. Politiske beslutningstakere har en forventning om at slike angrep blir forhindret, samtidig som rettssikkerhet, herunder den enkeltes personvern, skal ivaretas. Dette handler om å balansere ulike hensyn som trekker i forskjellige retninger, nulltoleranse for terrorangrep på den ene siden og ønsket om å bevare rettsstaten tuftet på demokratiske verdier på den annen.

Domstolskontroll er den sikreste mekanismen for å kontrollere at lover ikke gis for vid anvendelse. Hensikten er å hindre formålsutglidning, og at rettsstatens fundament ikke blir rokket ved. Som tidligere fremhevet, er det et generelt vilkår for bruk av tvangsmidler at anvendelsen ikke fremstår som et uforholdsmessig inngrep, og dette gjelder uavhengig av om det er politiet, påtalemyndigheten eller domstolen som har kompetansen til å beslutte bruk av det aktuelle tvangsmiddel. Domstolskontroll sikrer også kontradiksjon og at den mistenkte/siktede har nødvendig rettslig bistand.

7.2.4 Behandling av personopplysninger i domstolene og kriminalomsorgen

Domstolene og kriminalomsorgen behandler personopplysninger til ulike formål, basert på ulike lover, forskrifter eller instrukser. I det følgende gis det en kort og summarisk oversikt over relevant regelverk.

7.2.4.1 Domstolene

Domstolene behandler personopplysninger både ved forvaltningsmessige formål og i forbindelse med dømmende virksomhet. Forvaltningsmessige formål omfatter for eksempel å besvare generelle henvendelser fra publikum, oppbevaring av testamenter og administrering av aktører i rettssystemet som meddommere, tolker og bistandsadvokater. Behandling av personopplysninger for forvaltningsmessige formål i domstolen reguleres av personopplysningsloven.

Dømmende virksomhet er unntatt fra personopplysningslovens virkeområde, og reguleres blant annet av domstolloven, straffeprosessloven og tvisteloven.[31] Arkivloven regulerer hvordan opplysningene skal lagres og når de skal slettes.[32]

Domstolsadministrasjonen (DA) ved direktøren er behandlingsansvarlig for DAs behandling av personopplysninger. Hver domstol utgjør en egen selvstendig organisasjon. Det er dermed den enkelte domstol som er behandlingsansvarlig for behandlingen av personopplysninger i forbindelse med den enkelte domstols dømmende virksomhet. For ikke-dømmende virksomhet i den enkelte

---

[27] Formålet med etterforskningen er å avklare om det har funnet sted et straffbart forhold og å innhente de opplysninger som er nødvendig for sakens påtalemessige avgjørelse og eventuelle behandling i rettsapparatet. Etterforskning er et rettslig begrep som må avgrenses mot annen virksomhet som blir utført av politiet.
Avgrensningen av etterforskningsbegrepet har særlig betydning for hvem som har ansvaret for behandlingene som foretas.

[28] Personopplysningsloven § 2 jf. personvernforordningen art. 2.

[29] Se eksempelvis: Personvernforordningen art. 5 bokstav c og politiregisterloven § 8 om sletting/begrensing av behandling. I tillegg, personvernforordningen art. 9 og politiregisterloven § 7 om særlige kategorier av personopplysninger.

[30] Grunnloven § 96 og EMK artikkel 7 nr 1.

[31] Personopplysningloven § 2 annet ledd bokstav b.

[32] Lov 4. desember 1992 nr. 126 om arkiv (arkivlova).

domstol, har Domstolsadministrasjonen og den enkelte domstol felles behandlingsansvar.[33]

Det er oppnevnt et felles personvernombud for domstolene, Domstolsadministrasjonen og andre tilhørende organer. Personvernombudet er ombud for behandlingen av personopplysninger som omfattes av personvernforordningen, det vil si oppgaver av forvaltningsmessig karakter. Behandling av personopplysninger i forbindelse med domstolenes dømmende virksomhet faller utenfor personvernombudets arbeidsområde.

7.2.4.2 Kriminalomsorgen

For behandling av personopplysninger i kriminalomsorgen gjelder personopplysningsloven med utfyllende regler fastsatt i straffegjennomføringsloven.[34] I tillegg er det særlige regler for behandling av personopplysninger i IT-systemet INFOFLYT.[35] Dette systemet deler informasjon med politiet og gir kriminalomsorgen behandlingsgrunnlag til slik deling av personopplysninger.[36]

Kriminalomsorgen består i dag av kriminalomsorgsdirektoratet, regionalt nivå, og lokale enheter (fengsel, overgangsbolig og friomsorgskontor), samt kriminalomsorgens it-tjeneste. Det følger ikke eksplisitt av straffegjennomføringsloven hvilket organ innad i kriminalomsorgen som har behandlingsansvar. Det følger av forarbeidene til loven at behandlingsansvaret bør plasseres der behandling skjer og at den konkrete oppgavefordelingen må fastsettes i forskrift eller lov.[37] Videre kan det daglige behandlingsansvaret i følge forarbeidene delegeres. Det finnes ingen forskrift som fastsetter slik oppgavefordeling som nevnt i forarbeidene. I følge personvernerklæringen på kriminalomsorgens hjemmesider er det Kriminalomsorgsdirektoratet som har behandlingsansvar for behandling av personopplysninger i kriminalomsorgen.[38] I september 2021 sendte Datatilsynet en forespørsel til Kriminalomsorgsdirektoratet om utredning av behandlingsansvaret innenfor Kriminalomsorgen. Direktoratet ble pålagt å utarbeide en behandlingsprotokoll, samt å fremlegge internkontroll og dokumentasjon som viser hvordan behandlingsansvaret er plassert i hele etaten.[39] Datatilsynet gjennomførte deretter tilsyn med Kriminalomsorgsdirektoratet i november 2021.

Kriminalomsorgen er sammensatt og en stor sektor med 58 operative fengsler og rundt 5000 ansatte. Som nevnt i forarbeidene skal behandlingsansvar legges der behandlingen skjer, men det synes som det utelukkende er kriminalomsorgsdirektoratet som står som behandlingsansvarlig. Hjemmesidene til de ulike fengslene har ingen informasjon om behandlingsansvar. Justis- og beredskapsdepartementet har varslet at de er i gang med arbeidet med ny lov om behandling av personopplysninger ved straffegjennomføring. *Personvernkommisjonen* stiller spørsmål om kriminalomsorgen har foretatt relevante og nødvendige vurderinger for å avklare og plassere behandlingsansvaret for behandling av personopplysninger om innsatte.

Personvernkommisjonen mener Justis- og beredskapsdepartementet i arbeidet med ny lov om straffegjennomføring, bør tydeliggjøre behandlingsansvaret i kriminalomsorgen og legge ansvaret til den virksomhet som utfører den faktiske behandlingen av personopplysninger.

Straffegjennomføringsloven regulerer Datatilsynets tilsynskompetanse overfor kriminalomsorgen. Dersom det er besluttet unntak fra innsynsretten av kriminalomsorgen eller politiet, skal kriminalomsorgen ikke tilkjennegi at det foreligger registrering og Datatilsynet kan heller ikke gi pålegg om innsyn.[40] Datatilsynets tilsynskompetanse er dermed noe begrenset sammenlignet med kompetansen gitt etter personopplysningsloven og personvernforordningen.

7.3 Utviklingstrekk som påvirker personvernet

Den gjennomgående digitaliseringen av samfunnet, og den omfattende mengden av data som samles og brukes, har hatt stor påvirkning på justis-

[33] Norges Domstoler (u.å.). *Personvern i domstolene og Domstoladministrasjonen*.

[34] Se Lov 18. mai 2001 nr. 149 om gjennomføring av straff mv. (straffegjennomføringsloven) kapittel 1A, § 4a.

[35] Se straffegjennomføringsloven kapittel 1B.

[36] INFOFLYT ble etablert i 2005 og er et system for gjensidig utveksling av informasjon mellom kriminalomsorgen og politiet/påtalemyndigheten. Systemet skulle gi kriminalomsorgen et bedre grunnlag for å sikkerhetsvurdere varetektsfengslede og dømte. Den informasjonen som registreres gjelder innsatte som antas å medføre særlig rømningsfare, fare for anslag utenfra for å bistå til rømning, gisseltaking og fare for ny særlig alvorlig kriminalitet. Videre omfatter informasjonen innsatte med spesielt beskyttelsesbehov og innsatte som kan ha tilhørighet til organiserte kriminelle nettverk. Innst. 243 S (2011–2012). INFOFLYT er regulert i Justisdepartementets rundskriv G-3/2005.

[37] Prop. 151 L (2009–2010) *Endringar i forvaltningslova og straffegjennomføringslova,* side 38.

[38] Kriminalomsorgen. (u.å.). *Personvernerklæring.*

[39] Datatilsynet. (2021). *Vedtak om pålegg til Kriminalomsorgsdirektoratet.*

[40] Se straffegjennomføringsloven § 4j tredje ledd.

sektoren. Utviklingen åpner for informasjonsinnhenting i stor skala, samtidig som nye analysemetoder bidrar til at politiet kan arbeide på nye måter.

Parallelt med digitaliseringen har det også blitt gjennomført en rekke lovendringer som skal tilrettelegge for kriminalitetsbekjempelse i det digitale samfunnet. Sammensetningen av nye metoder for kriminalitetsbekjempelse og utvidede lovhjemler for informasjonsinnhenting kan sette personvernet under press. Det gjelder for mistenkte og pårørende i straffesaker, men også for utenforstående og samfunnet som helhet. Nedenfor vil *Personvernkommisjonen* søke å gjøre rede for denne utviklingen, og belyse hvordan den påvirker personvernet. Mer inngående drøftelser av personvernutfordringene gjøres i avsnitt 7.4.

7.3.1 Endringer i kriminalitetsbildet

Kriminalitetssituasjonen er i stadig endring, og i likhet med andre deler av samfunnet flytter kriminaliteten seg i mange tilfeller over i digitale flater.[41] I politiets trusselvurdering 2022 beskrives det digitale trusselbildet som utfordrende, og et økende omfang av blant annet datainnbrudd, spredning av overgrepsmateriale, løsepengevirus og ekstreme ytringer omtales som noen av de mest alvorlige digitale truslene.[42] Politiet må etterforske både lokale saker og saker med internasjonale forgreininger eller opprinnelse.

Arbeidet for å forhindre og oppklare seksuelle overgrep mot barn over internett har blitt prioritert av norsk politi i den senere tid. Det er et kriminalitetsområde som er i konstant økning blant annet fordi bilder og film med overgrep mot barn ikke blir borte. Materialet deles igjen og igjen, og øker i omfang. Det er uvisst hvor stort omfanget av denne kriminaliteten er, men det kan legges til grunn at det er omfattende. Oppdagelsesrisikoen er dessuten lav.[43] Etterforskning av denne typen saker er et område hvor personvernet kommer under særlig press, da formålet om å bekjempe seksuelle overgrep mot barn fordrer bruk av potensielt svært inngripende metoder.

Økning i saker som gjelder digital kriminalitet krever økte ressurser og spesialkompetanse. Etterretning og avdekking, forebygging, metode- og regelverksutvikling, samt etterforskning og iretteføring av digital kriminalitet forutsetter en effektiv organisering av arbeidet i politiet, og tett samarbeid med andre relevante aktører i samfunnet.[44]

Det endrede kriminalitetsbildet merkes også i domstolene. Teknologiutviklingen har ført til at nye sakstyper er kommet til og at mer tradisjonell vinningskriminalitet synes å bli erstattet av nettbasert kriminalitet. Det samme gjelder omfattende seksuallovbruddsaker der de straffbare forholdene er utført på nett.[45]

7.3.2 Økt internasjonalt samarbeid

Økt kriminalitet på tvers av landegrenser som følge av digitaliseringen, øker behovet for internasjonalt samarbeid. Dette gjelder særlig politiarbeidet. Ofte er for eksempel lagringsenhetene hvor relevante opplysninger ligger lagret, den kriminelle aktøren og offeret lokalisert i forskjellige land. Derfor er forebygging og bekjempelse av kriminalitet nasjonalt og lokalt i mange tilfeller avhengig av at norsk politi bidrar til og deltar i internasjonalt samarbeid.[46] Utlevering av personopplysninger til andre aktører og mottakere i utlandet er en naturlig del av dette samarbeidet.[47] På tvers av landegrensene skjer samarbeidet i praksis gjennom en av flere formaliserte mekanismer, som for eksempel gjennom EUROPOL eller INTERPOL. Ved deltagelse i internasjonalt samarbeid er det en forutsetning at nasjonale lover og regler følges.

EUROPOL ble etablert i 1999 og ga grunnlag for samarbeid mellom EU-landene i møte med transnasjonal kriminalitet. Norge har hatt en samarbeidsavtale med EUROPOL siden 2001. Behandling av personopplysninger som en del av EUROPOL-samarbeidet reguleres gjennom EU-forordning 2016/794.[48]

INTERPOL er det eneste verdensomspennende politisamarbeidet, med 194 medlemsland.[49]

---

41 Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden.* Justis- og beredskapsdepartementet. Side 10.

42 Politiet. (2021). *Politiets trusselvurdering 2021.*

43 Kripos. (2019). *Seksuell utnyttelse av barn og unge over internett.*

44 Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden.* Justis- og beredskapsdepartementet.

45 Norges Domstoler. (2020). *Årsrapport 2020.*

46 Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden.* Justis- og beredskapsdepartementet, s. 45.

47 Se politiregisterloven § 22 for hjemmel for utlevering av opplysninger til utlandet.

48 I desember 2020 har Europakommisjonen fremmet et forslag om å fornye EUROPOL forordningen (2016/794), ved å legge bedre til rette for offentlig- privat samarbeid for å forebygge, avdekke og motarbeide alvorlig kriminalitet. Kommisjonen ønsker i tillegg å tillatte gjenbruk av personopplysningen e som EUROPOL besitter for å fremme forskning og innovasjon, samt øke EUROPOLs evne til å gi operativ bistand i pågående etterforskning i medlemsland. EDPS. (2021). *Opinion 4/2021: EDPS Opinion on the proposal for amendment of the Europol regulation.*

Det ligger ingen folkerettslig bindende konvensjon til grunn for organisasjonen, men vilkåret for å bli medlem, er at landet anerkjenner FNs menneskerettserklæring. INTERPOLs fremste oppgave er å formidle informasjon, bistandsanmodninger og rettsanmodninger mellom medlemslandenes myndigheter.

7.3.3 Nye verktøy og metoder

Digitaliseringen av kriminalitetsbildet innebærer at justissektoren må ta i bruk nye verktøy og metoder for å kunne oppfylle sitt samfunnsoppdrag og sørge for effektiv kriminalitetsbekjempelse.[50] Teknologiutviklingen skaper nye muligheter for å oppnå tryggere, raskere og mer effektiv kriminalitetsbekjempelse. Samtidig har teknologiutviklingen ført til at det registreres enorme mengder informasjon om samtlige innbyggere. Tilgangen og muligheten til å analysere denne informasjonen vil være relevant for justissektorens arbeid i flere sammenhenger. Samtidig er det behov for sterke juridiske, tekniske og organisatoriske kontrollmekanismer for å sørge for at bruken av informasjonen skjer innenfor forsvarlige rammer.

Hvordan ulike land anvender nye teknologier, under hvilke premisser, og med hvilke rettsikkerhetsgarantier, er et rettspolitisk spørsmål. Mange av metodene andre land allerede har tatt i bruk i arbeidet med kriminalitetsbekjempelse, vil det før eller siden også bli reist spørsmål ved om vi bør anvende i Norge. Bruk av kraftigere verktøy kan føre til at metodebruken blir mer inngripende i innbyggernes personvern, ikke bare for parter i en sak, men for befolkingen i sin helhet. Dette gjelder særlig dersom innsamlede opplysninger vurderes som relevant for oppgaveløsning utenfor innsamlingsformålet og i nye kontekster, eller ved omfattende datainnsamling om store deler av befolkningen som en del av et analysearbeid.

En effektiv justissektor er avhengig av tilgang til store mengder informasjon fra mange ulike kilder, for å fatte kunnskapsbaserte og godt begrunnede beslutninger. Informasjon benyttes til å understøtte beslutninger for å forebygge og bekjempe kriminalitet, blant annet for å vurdere antatt farepotensiale, eller i utvelgelse av tiltak, for eksempel å ilegge en fengselsstraff. Innhenting av informasjon skjer for eksempel som et ledd i etterforskning, der politiet sammenstiller og danner et bilde av en trussel eller en kriminell handling. Dette kan innebære inngrep i borgernes rett til personvern, som drøftet nedenfor i avsnitt 7.4.5.

7.3.4 Politiske føringer – utvidelser av politimyndighetenes inngrepsmuligheter

Det er en overordnet politisk målsetning og en samfunnsmessig forventning at politiet og påtalemyndighetene skal være i stand til å bekjempe og forebygge alvorlig kriminalitet. I takt med teknologiutviklingen dukker det jevnlig opp nye situasjoner som gjør det krevende for politiet å utføre sitt arbeid, for eksempel ved at en ny teknologi gjør det vanskeligere å avdekke kriminelle nettverk. Når slike situasjoner oppstår, vil det ofte innebære ønsker om nye eller utvidede hjemler for å sette politiet i stand til å utføre sine oppgaver i det endrede teknologilandskapet. For eksempel har det ved gjentatte tilfeller vært diskutert om politiet bør ha tilgang på såkalte bakdører inn i krypterte meldingstjenester, da teknologien gjør det mulig å skjule alvorlig kriminalitet. Samtidig kan slike bakdører skape nye sårbarheter, da disse kan misbrukes av andre aktører.[51]

Det har vært en utvikling over tid med utvidelser av politimyndighetenes hjemler til å bedrive skjult kontroll med, og overvåkning av, blant annet borgernes elektroniske kommunikasjon. Utvidelsene har i stor grad kommet stykkevis og delt. Dette har trolig medført at hverken myndighetene eller borgerne har vært i stand til å over-

Boks 7.2 Eksempel på analyseverktøy

Politihøgskolen og NTNU Gjøvik samarbeider om et prosjekt kalt «Ars Forensica». I dette prosjektet undersøkes bruken av forskjellige former for kunstig intelligens i analyse av stordata, med formål om å avdekke, forebygge og etterforske økonomisk kriminalitet. Målet med prosjektet er å «gi ny kunnskap som forbedrer forebygging, etterforskning og påtale av hendelser, samtidig som hensyn til personvern og rettssikkerhet ivaretas».[1]

[1] Kommunal- og distriktsdepartementet. (2020). *Nasjonal strategi for kunstig intelligens.*

[49] INTERPOL. (u.å.). *What is INTERPOL?*

[50] Politiets samfunnsoppdrag er definert i Meld. St. 42 (2004–2005) *Politiets rolle og oppgaver.* Justis- og beredskapsdepartementet.

[51] Digi. (2015, 25. mai). *Advarer mot politiets drøm om bakdør.*

skue sammenhengen mellom alle de ulike hjemlene og konsekvensene av utvidelsene.

Reguleringen er spredt over flere lover, og kan være utfordrende å få oversikt over. Enkelte hjemler finnes i politiloven, andre i straffeprosessloven. Hjemlene er knyttet til forebygging og/eller etterforskning av straffbare handlinger, som igjen er regulert og definert i straffeloven.

Når det gjøres enkeltstående endringer i lovgivningen er det komplisert å få oversikt over konsekvenser, herunder konsekvenser for personvernet. Mangel på oversikt kan videre føre til at det blir vanskeligere å sørge for solid demokratisk kontroll over lovprosessene.

Ulike EU-regelverk legger også en rekke politiske føringer for justissektoren, som kan ha personvernkonsekvenser for norske innbyggere. Disse føringene behandles ikke inngående her. *Personvernkommisjonen* trekker kun frem et eksempel for å illustrere at utviklingen på europeisk nivå også kan legge press på personvernet. I mars 2022 la Europakommisjonen frem forslag til en ny lov som har som formål å oppdage og stoppe spredning av overgrepsmateriale av barn på nett.[52] I lovforslaget legges det blant annet vekt på at tjenestetilbydere må avdekke om deres tjenester brukes til spredning av overgrepsmateriale, og rapportere dette til nasjonale politimyndigheter. Flere eksperter på personvern og IKT-sikkerhet har varslet om at forslaget kan innebære at all privat digital kommunikasjon blir gjenstand for skanning. Dette kan undergrave muligheten til konfidensiell kommunikasjon på nett.[53]

Politiske føringer for det europeiske politisamarbeidet gjennom EUROPOL kan også skape personvernutfordringer. I 2020 avdekket datatilsynsmyndigheten for EU-organene (EDPS) i et tilsyn at EUROPOL mottar stadig større mengder personopplysninger fra politiet i medlemslandene og at behandlingen av disse opplysningene ofte er i strid med personvernregelverket.[54] Det kom blant annet fram at EUROPOL mottar store mengder overskuddsinformasjon fra medlemslandene. Dette er informasjon som de ikke har adgang til å lagre og behandle i henhold til forordning 2016/794,[55] men som de heller ikke har mulighet til å filtrere bort eller avvise å ta imot, idet den er sendt ut av politiet i et medlemsland. I følge tilsynsrapporten stiller dette høye krav til bevissthet og kunnskap fra samarbeidende medlemsland. I tillegg bør det foreligge en mulighet for disse til å filtrere bort irrelevant informasjon før den lastes opp i EUROPOL sine datasystemer. EDPS anbefaler videre at EUROPOLs rolle som databehandler for politiet i medlemslandene avklares og formaliseres.

I 2022 kom det fram at Rådet i EU har lagt fram et forslag om lovendringer for å utvide EUROPOLs muligheter til å behandle store mengder personopplysninger, i strid med anbefalingene fra EDPS.[56] Dette har blitt kritisert som en inngripende utvidelse av EUROPOLs mandat som tilsidesetter EDPS sin autoritet som tilsynsmyndighet.[57] En mulig følge av forslaget vil være at stadig flere personopplysninger om europeiske innbyggere vil kunne behandles i grensekryssende etterforskningssaker.

Personvernkommisjonen mener funnene EDPS har avdekket om at EUROPOL mottar store mengder personopplysninger fra politiet i medlemsland, må følges opp av norske myndigheter for å sikre at personvernet til norske innbyggere blir ivaretatt når politiet overfører opplysninger til EUROPOL. *Kommisjonen* antar at tilsvarende problemstillinger kan foreligge i andre sammenhenger hvor opplysninger utveksles mellom politimyndigheter, for eksempel mellom Norge og INTERPOL, og dette også må følges opp.

7.4 Personvernutfordringer i justissektoren

I noen tilfeller vil det, som nevnt ovenfor, være et spenningsforhold mellom formål knyttet til kriminalitetsbekjempelse og -forebygging, og innbyggernes rett til personvern. Aktører i justissektoren vil kunne ha et ønske om å kunne ta i bruk nye metoder og verktøy for å utføre sine samfunnsoppdrag, og dette kan ha effekter på personvernet til både parter i en bestemt sak, individer som ikke er direkte involvert i en sak, og for grupper i samfunnet.

I det følgende trekker *Personvernkommisjonen* frem det *kommisjonen* anser som de viktigste utfordringene for personvernet i justissektoren.

---

52 European Commission. (2022). *Questions and Answers – New rules to fight child sexual abuse*.

53 European Digital Rights. (2022, 11. mai). *Private and secure communications attacked by European Commission's latest proposal*.

54 European Data Protection Supervisor. (2020, 5. okotober). *EDPS Decision on the own initiative inquiry on Europol's big data challenge*.

55 Europol-forordningen, se kapittel IV om behandling av personopplysninger.

56 Statewatch. (2022, 25. januar). *Europol: Council Presidency proposes workaround for illegal data processing.*

57 European Digital Rights. (2022, 31. januar). *Secret negotiations about Europol: the big rule of law scandal*.

Noen av disse problemstillingene er direkte knyttet til eksisterende lovverk og prosedyrer i sektoren, mens andre er av overordnet, prinsipiell karakter.

Kommisjonen har valgt å dele opp utfordringene i flere underkapitler. Problemstillingene som drøftes vil nødvendigvis ha overlappende elementer. For eksempel vil ufullstendige personvernvurderinger henge sammen med manglende personvernkompetanse, og utvikling av ny teknologi kan føre til forslag om lovendringer.

Først vil *kommisjonen* beskrive hvordan vurdering av personvernkonsekvenser, både på systemnivå (mengden av tiltak sett under ett) og i konkrete saker, bør få en mer fremtredende rolle i lovarbeid. *Kommisjonen* kommenterer også utfordringer knyttet til ivaretakelsen av personvernet i forbindelse med myndighetsutøvelse.

Ny teknologi, som maskinlæringssystemer som har som formål å forutsi kriminalitet, kan være effektive verktøy i kriminalitetsbekjempelse. *Personvernkommisjonen* vil se på hvilke potensielle personvernkonsekvenser bruk av slik teknologi kan ha for den enkelte, og for samfunnet i stort.

Dersom det foreligger mangel på åpenhet og demokratisk kontroll som følge av nye metoder er dette i seg selv problematisk. *Kommisjonen* vil også drøfte utfordringer ved svakheter knyttet til enkelte systemer og verktøy for å ivareta personvernet på en effektiv måte i justissektoren. Avslutningsvis vil *kommisjonen* se på kontrollmekanismene som skal ivareta personvernet i sektoren, og peke på mulige svakheter og forbedringspunkter ved disse.

7.4.1 Personvern i lovarbeid

Personvernkommisjonen anerkjenner behovet for å forebygge og bekjempe kriminalitet i en digitalisert verden. *Kommisjonen* er likevel bekymret for at personvernet kan bli tilsidesatt for å oppnå disse målene, uten at det foretas tilstrekkelige vurderinger og interesseavveininger.

Ved innføring av nye tiltak er det avgjørende at eventuelle personvernkonsekvenser blir tilstrekkelig belyst og vurdert i forkant. Lovgiver skal begrunne tiltakenes nødvendighet og proporsjonalitet i tråd med menneskerettslige forpliktelser og eksisterende lovverk.

Et kriminalitetsbilde i stadig endring og utvikling av nye verktøy kan skape behov og ønsker om å endre eksisterende lovverk eller introdusere nye hjemler for å muliggjøre effektiv kriminalitetsbekjempelse og forebygging. I mange tilfeller vil slike endringer utgjøre inngrep i og begrense retten til personvern. Derfor må det være en forutsetning at det utføres grundige utredninger av mulige personvernkonsekvenser i lovarbeid. En slik plikt følger også av Utredningsinstruksen med tilleggsveileder, se nærmere omtale av vurderinger av personvernkonsekvenser i lovarbeid i kapittel 6.

Personvernkommisjonen har observert at vurderinger av personvernkonsekvenser kan være begrensede og mangelfulle i forbindelse med nye lov- og forskriftsforslag. Det synes også å være slik at *samlede effekter* ved innføring av flere inngripende forslag får for liten oppmerksomhet

Som nevnt innledningsvis har skiftende regjeringer de siste årene fremmet en rekke forslag til lov- og/eller forskriftsendringer, med betydelige konsekvenser for borgernes personvern. Dette inkluderer blant annet forslag om å gi politiet utvidet adgang til å benytte skjulte tvangsmidler (herunder kommunikasjonskontroll og dataavlesning),[58] forslag om å utvide forsvarets tilgang til politiets registre, forslag som kriminaliserer samarbeid med fremmed etterretningstjeneste om å utøve påvirkningsvirksomhet,[59] forslag til endringer i e-komloven (med utvidet lagring av IP-adresser), forslag om politiets tilgang til utlendingsmyndighetenes registre, forslag om systematisk registrering av flypassasjerer,[60] og forslag om endringer i lovverket for å gi PST hjemmel til å lagre, systematisere og analysere opplysninger fra åpne kilder på internett.[61]

En gjennomgående svakhet i vurderingene som gjøres, er at de ikke inneholder en forholdsmessighetsvurdering av tiltaket, det vil si hva de konkrete endringene innebærer for innbyggernes grunnleggende rettigheter. Forholdsmessighetsvurderingene inneholder ofte lite annet enn en påpekning av at muligheten for å bekjempe alvorlig kriminalitet i samfunnet vil svekkes dersom politi og påtalemyndighet ikke sikres tilgang til data. Det er også en gjennomgående svakhet at det ikke gjøres reelle vurderinger av tiltakets nød-

---

58 Prop. 68 L (2015–2016) *Endringer i straffeprosessloven mv. (skjulte tvangsmidler)*

59 Justis- og beredskapsdepartementet. (2021). *Høring om endringer i straffeloven mv. – påvirkningsvirksomhet.*

60 Justis- og beredskapsdepartementet. (2021). *Høring – endringer i grenseloven mv., ny forskrift om grensetilsyn og grensekontroll av personer (grenseforskriften) mv. og nytt kapittel 60 i politiregisterforskriften om behandling av flypassasjerinformasjon (PNR-opplysninger)*.

61 Justis- og beredskapsdepartementet. (2021). *Høring – Endringer i politiloven og politiregisterloven mv. – PSTs etterretningsoppdrag og behandling av åpent tilgjengelig informasjon*.

vendighet. I flere tilfeller legges det til grunn at tiltakene er effektive og nødvendige sett opp imot politiets behov. Effektiviteten diskuteres i liten grad kritisk. I stedet for å gjøre forholdsmessighets- og nødvendighetsvurderinger, peker lovgiver på betydningen av rettssikkerhetsgarantier og at disse ivaretar hensynet til borgernes rettssikkerhet og personvern.

Personvernkommisjonen vil i det følgende trekke frem noen eksempler fra lov- og forskriftsarbeid der mangler ved vurderingen av personvernkonsekvenser har blitt påpekt:

- I 2016 introduserte Samferdselsdepartementet et forslag om en endring i vegtrafikkloven for å gi politiet direkte tilgang til motorvognregistret, førerkortregistret og bilde- og signaturregistret til bruk for politimessige formål. I sitt høringssvar stilte Datatilsynet seg kritisk til det de beskriver som en «utvikling hvor stadig flere registre stilles til disposisjon for andre formål enn de ble opprettet for». Tilsynet argumenterte for at et ønske om slike utvidede hjemler burde fremmes som eget lovforslag for å opprette et nytt register, for å sikre en grundig politisk prosess.[62] Tilsynet fikk begrenset gehør for sine synspunkter, og politiet fikk tilgang til motorvognregistret og førerkortregistret.
- I 2018 la Justis- og beredskapsdepartementet fram et forslag om å opprette et nasjonalt register over drap og vold med dødelig utgang. I sin høringsuttalelse påpekte Datatilsynet at opplysninger om døde personer anses som personopplysninger dersom de kan knyttes til en levende person. Datatilsynet kritiserte forslaget for å ikke ha gjort tilstrekkelige vurderinger av personvernkonsekvenser for pårørende.[63] Forslaget var i juli 2022 fortsatt til behandling.
- I 2018 publiserte Justis- og beredskapsdepartementet en høring om utveksling av personopplysninger i forbindelse med bekjempelse av arbeidslivskriminalitet. Forslaget inkluderte en ny bestemmelse i personopplysningsloven for å gi hjemmel for utvekslingen av personopplysninger mellom offentlige organer i forbindelse med arbeid med å bekjempe arbeidslivskriminalitet. Datatilsynet og Difi kritiserte blant annet høringsnotatet for å ikke vurdere hvilke implikasjoner forslaget ville kunne få for personvernet.[64]
- I 2021 sendte Justis- og beredskapsdepartementet ut en høring om endringer i straffeloven, straffeprosessloven og politiloven for å kriminalisere samarbeid med fremmede etterretningstjenester som kan utgjøre påvirkningsvirksomhet. Blant annet Advokatforeningen, Den internasjonale juristkommisjon og Datatilsynet kritiserte i sine høringssvar forslaget for å ikke tilstrekkelig utrede personvern- og ytringsfrihetskonsekvenser.[65]
- I 2021 publiserte Justis- og beredskapsdepartementet en høring om forslag til ny grenseforskrift, samt endringer i grenseloven, politiregisterloven, utlendingsloven og grenseforskriften. Forslaget omhandlet blant annet innsamling av informasjon om flypassasjerer, inkludert lagring av personopplysninger i fem år. Tekna, Datatilsynet og Norges Institusjon for Menneskerettigheter kritiserte forslaget for å ikke drøfte personvernkonsekvenser av forslaget i høringsnotatet.[66] Datatilsynet påpekte også at tilsynet ikke var blitt konsultert av departementet før høringsnotatet ble lagt fram.
- I 2021 sendte Kommunal- og moderniseringsdepartementet og Justis- og beredskapsdepartementet på høring et forslag om endringer i ekomloven. Forslaget innebar å innføre plikt for tilbydere av ekomtjenester til å lagre IP-adresser, med formål om at politiet kan få tilgang som ledd i bekjempelsen av alvorlig kriminalitet. Forslaget ble blant annet kritisert av Abelia og Datatilsynet for å ikke gjøre en helhetsvurdering av personvernkonsekvenser i sammenheng med andre inngripende lovendringer. Forslaget ble også kritisert av blant annet Advokatforeningen, Den Internasjonale Juristkommisjon, Norsk Journalistlag og Tekna for å ikke tilstrekkelig vurdere proporsjonaliteten av inngrep opp mot personvern, ytringsfrihet og kildevern.[67] Datatilsynet

[62] Samferdselsdepartementet. (2016). *Høring – Vegtrafikkloven ny § 43 b – Rett til å behandle personopplysninger – politiets tilgang til personopplysninger i Statens vegvesens registre*.

[63] Datatilsynet. (2018). *Høringsuttalelse – Register over drap og vold med dødelig utgang*.

[64] Justis- og beredskapsdepartementet. (2018). *Høring – utveksling av personopplysninger i forbindelse med bekjempelse av arbeidslivskriminalitet*.

[65] Justis- og beredskapsdepartementet. (2021). *Høring om endringer i straffeloven mv. – påvirkningsvirksomhet*.

[66] Justis- og beredskapsdepartementet. (2021). *Høring – endringer i grenseloven mv., ny forskrift om grensetilsyn og grensekontroll av personer (grenseforskriften) mv. og nytt kapittel 60 i politiregisterforskriften om behandling av flypassasjerinformasjon (PNR-opplysninger)*.

[67] Kommunal- og distriktsdepartementet & Justis- og beredskapsdepartementet. (2020). *Høring – Endringer i ekomloven*.

bemerket også at departementene ikke hadde rådført seg med tilsynet før forslaget ble lagt fram.

– I 2021 sendte Justis- og beredskapsdepartementet på høring et forslag til endringer i politiloven, politiregisterloven og politiregisterforskriften.[68] Forslaget inkluderer endringer i lovverket for å gi PST hjemmel til å lagre, systematisere og analysere store mengder informasjon fra åpne kilder på internett, selv om den enkelte opplysning ikke er nødvendig for det angitte formålet. Informasjonen, som vil kunne angå «en stor andel av befolkningen», skal kunne lagres i 15 år. I følge departementet er det ikke praktisk gjennomførbart å sette begrensningskriterier for hvilke opplysninger som kan lastes ned, fordi det ved kartlegging av trusselbilder ikke på forhånd vil være sikkert hvilke data som kan være av betydning. Forslaget har møtt kritikk fra blant andre Advokatforeningen, Datatilsynet og Norsk Institusjon for Menneskerettigheter. Kritikken går blant annet på at forslaget synes å utgjøre et uforholdsmessig stort inngrep i personvernet til samtlige innbyggere uten at dette er tilstrekkelig begrunnet fra departementet, at det antageligvis strider mot rettspraksis fra EMD, samt at negative ringvirkninger på ytringsfriheten og personvernet ikke er tilstrekkelig utredet.[69]

Eksemplene over illustrerer at det er tydelige mangler ved vurderinger av personvernkonsekvenser i lov- og forskriftsarbeider. *Personvernkommisjonen* har inntrykk av at dette blant annet skyldes at Datatilsynet i liten grad involveres før personverninngripende lov- og forskriftsforslag sendes på høring.

Etter personvernforordningen artikkel 36 nr. 4 foreligger det et krav om at «Medlemsstatene skal rådføre seg med tilsynsmyndigheten ved utarbeiding av forslag til lovgivning som skal vedtas av et nasjonalt parlament, eller av et reguleringstiltak som er basert på slik lovgivning, og som er knyttet til behandling». *Personvernkommisjonen* mener, som kommentert i kapittel 6 og mer uførlig diskutert i kapittel 13, at rådføringsplikten ikke kan anses å være etterlevet ved å gi Datatilsynet anledning til gi innspill i forbindelse med en ordinær offentlig høringsprosess.

Personvernkommisjonen ser grunn til å stille spørsmål ved om rådføringsplikten etterfølges i tilstrekkelig grad av norske myndigheter i dag innenfor justissektoren.

Som en mulig følge av at personverninngripende høringsforslag ikke er gjenstand for rådføring med Datatilsynet, ser *kommisjonen* at høringsnotater ofte utilstrekkelig beskriver mulige personvernkonsekvenser. Dette kan videre føre til at viktige personvernhensyn ikke belyses som en del av saksgrunnlaget når lovforslag behandles i Stortinget. Eksemplet fra Danmark beskrevet nedenfor i avsnitt 7.4.5, illustrerer hvordan slike mangler i verste fall kan føre til at parlamentarikere ikke har grunnlag for å forstå konsekvensene for personvernet, ved innføring av nye lover og hjemler. Dette vil i så fall være et demokratisk problem.

En grundig vurdering av personvernkonsekvenser i lovarbeid er en forutsetning for demokratisk kontroll. I kapittel 6 anbefaler *Personvernkommisjonen* at regjeringen vurderer om rådføringsplikten følges i tilstrekkelig grad i dag, og hvordan denne plikten ev. bør innrettes for å ikke forsinke lovarbeidet unødig, samt føre til en uforholdsmessig stor ressursbelastning for Datatilsynet.

I flere av lovarbeidene hvor mulige personvernkonsekvenser faktisk berøres, formuleres disse konsekvensene som utfordringer for individers personvern. For eksempel kan en mulighet for at enkeltpersoner settes under mistanke på grunn av utvidede hjemler for datainnsamling, adresseres med at domstolskontroll og andre kontrollmekanismer vil kunne hindre at enkeltindivider utsettes for urettmessige inngrep i personvernet. Som beskrevet i kapittel 3 er det svakheter ved å formulere personvernkonsekvenser som et rent individuelt anliggende. Dersom personvernkonsekvensene ved et lov- eller forskriftsforslag fremstilles som et individuelt anliggende, risikerer man at bredere samfunnseffekter, for eksempel nedkjølingseffekter som utfordrer ytringsfriheten, ikke fanges opp som en reell konsekvens. Dermed løper man en risiko for at grunnleggende spørsmål ikke blir drøftet som en del av lovarbeidet.

Personvernkommisjonen mener regjeringen må bevilge midler til forskning på samfunnsmessige konsekvenser av overvåkningstiltak i justissektoren. Dette er viktig kunnskap for å være i stand til å gjøre helhetsvurderinger ved innføring av lovendringer.

---

[68] Justis- og beredskapsdepartementet. (2021). *Høring – Endringer i politiloven og politiregisterloven mv. – PSTs etterretningsoppdrag og behandling av åpent tilgjengelig informasjon*.

[69] Justis- og beredskapsdepartementet. (2021). *Høring – Endringer i politiloven og politiregisterloven mv. – PSTs etterretningsoppdrag og behandling av åpent tilgjengelig informasjon*.

7.4.2 Vurdering av personvern i myndighetsutøvelse

Ivaretakelse av personvernet i forbindelse med myndighetsutøvelse setter høye krav både til politiet som organisasjon og til den enkelte ansatte. Tydelige hjemler, veiledning, rutiner og kontrollmekanismer er viktige forutsetninger for at personvernet skal ivaretas i det daglige politiarbeidet. I det følgende vil *Personvernkommisjonen* diskutere utfordringer knyttet til uklare hjemler, bruk av åpne kilder, formålsutglidning og deling av data mellom politiet og andre myndigheter.

7.4.2.1 Implementering av politidirektivet i politiregisterloven

Politiet har plikt til å vurdere personvernkonsekvenser av tiltak før de iverksettes. I disse vurderingene er det nødvendig med en viss grad av skjønnsutøvelse. Dersom tiltak ikke er utredet tilstrekkelig i lovarbeidet, og/eller hjemlene er uklare, kan dette føre til for stor grad av skjønn. Resultatet kan bli lite forutberegnelig og ramme skjevt, og over tid foreligger risiko for formålsutglidning.

Etter *kommisjonens* syn er politiregisterloven et eksempel der loven ikke oppstiller tilstrekkelige konkrete krav og føringer for behandling av personopplysninger. Loven bør forenkles og forbedres.

Det er behov for vurderinger av politiregisterlovgivningens harmonisering med EU-retten. EUs sektordirektiv 2016/680,[70] heretter politidirektivet, inneholder flere krav som ikke eksplisitt er gjennomført i politiregisterloven. Det gjelder for eksempel bestemmelser om vurderinger av automatiserte beslutningsprosesser[71] og innebygd personvern.[72] Kripos har pekt på at manglende gjennomføring av bestemmelsene kan medføre uklarhet rundt rettstilstanden når politiet skal vurdere bruk av ny teknologi, og hva som er tillatt når enkelte bestemmelser ikke er eksplisitt gjennomført i norsk rett. Videre kan det skape utfordringer i praksis at kravet til behandlingsgrunnlag ikke gjenfinnes i politiregisterloven.

Datatilsynet mener det er usikkert om regelverket som regulerer PSTs innhenting og bruk av personopplysninger inneholder tilstrekkelige hjemler til å benytte personopplysninger til utvikling av maskinlæringssystemer.[73]

Politiregisterloven mangler også bestemmelser som gjennomfører politidirektivet artikkel 4 om personvernprinsipper. Politidirektoratet ga i sitt høringssvar til *Personvernkommisjonens* mandat uttrykk for at det bør utformes en egen bestemmelse i politiregisterloven som gjennomfører politidirektivet artikkel 4 om prinsipper: «En egen bestemmelse om prinsipper vil i større grad bidra til harmonisering og brukervennlighet. Vi er også usikre på hvorfor ikke alle personvernprinsippene er gjennomført i politiregisterloven. Vi trekker særlig frem rettferdighetsprinsippet, som er et av de mest sentrale personvernprinsippene.»[74]

Videre er ikke politidirektivets artikkel 10 bokstav c implementert i politiregisterloven. Bestemmelsen gir hjemmel for politiets bruk av særlige kategorier personopplysninger som den registrerte selv har offentliggjort, som ikke gjenfinnes i politiregisterloven.[75] I lys av den teknologiske utviklingen og det store omfanget av tilgjengelige personopplysninger på Internett, er dette et praktisk viktig grunnlag som gir føringer for politiets bruk av slike opplysninger. I høringsnotatet uttalte departementet: «At den registrerte selv har offentliggjort slike opplysninger bør ikke være et selvstendig grunnlag for politiets behandling når vilkårene om formålsbestemthet og nødvendighet ikke er oppfylt».[76] Som følge av at denne bestemmelsen ikke er implementert i norsk lov, er ikke politiets rammer for, og adgang til å benytte informasjon fra åpne kilder (Facebook ol.) utredet og avklart gjennom en åpen og demokratisk debatt.[77] Politiets innhenting og bruk av personopplysninger fra åpne kilder i etterforskningssammenheng, vil bli diskutert i avsnittet under.

Kripos har gitt uttrykk for at det er en fordel om nevnte krav gjenfinnes i det norske regelverket, noe som også kunne bidratt til å gjøre kravene til personvernvurderinger klarere for de som bruker regelverket.

Personvernkommisjonen mener Justis- og beredskapsdepartementet må vurdere om alle

---

70 Direktiv 2016/680, (politidirektivet).

71 Jf. politidirektivet artikkel 11.

72 Jf. politidirektivet artikkel 20.

73 Datatilsynet. (2022). *Høringssvar om EOS-utvalgets behandling av personopplysninger*.

74 Politidirektoratet. (2018). *Høringssvar om mandat til personvernkommisjon*.

75 Jf. politidirektivet art. 10 bokstav c.

76 Justis- og beredskapsdepartementet. (2016). *Høring – endringer i politiregisterloven og politiregisterforskriften – implementering av direktiv (EU) 2016/680*.

77 Norsk politi fikk i 2018 etablert en nasjonal standard som beskriver metoder for innhenting av åpent tilgjengelig informasjon på internett til politimessige formål. Denne standarden er utarbeidet av Kripos for intern bruk i Politiet.

bestemmelsene i politidirektivet skal implementeres i politiregisterloven. En harmonisering av loven med direktivet vil gi klarere retningslinjer for personvernvurderinger og gjøre det enklere for tjenestepersoner å anvende loven.

7.4.2.2 Bruk av åpne kilder

Det produseres, lagres og utveksles enorme mengder personopplysninger digitalt, særlig gjennom sosiale medier og digitale plattformer. At mange «lever» en stor del av sine liv på nett, gjør også at den informasjonen som finnes der kan oppfattes som relevant i oppklaring av kriminalitet. Før var det mulig for politiet å etterforske for eksempel økonomisk kriminalitet, ved kun å ta beslag i mapper og permer som var relatert til en persons økonomiske virksomhet. Ved å ta beslag i en mobiltelefon eller datamaskin, er det mulig å få innsikt i svært mye om en persons liv og handlinger.

Lovkravene til innhenting og behandling av personopplysninger er de samme slik de fremgår av straffeprosessloven og politiregisterloven, og omfanget av tilgjengelig informasjon endrer ikke kravet til at informasjonen må ha betydning som bevis, eller eksempelvis oppfylle formålet om forebygging av lovbrudd i politiregisterloven § 47-1.

Informasjonsinnhenting fra åpne kilder på internett er en metode som kan benyttes til politimessige formål, herunder kriminalitetsbekjempelse i form av etterretningsvirksomhet, etterforskning og forebygging.

Det er flere problemstillinger politiet må hensynta ved informasjonsinnhenting fra åpne kilder på nett, og det første er om informasjonsinnhentingen foregår som del av en etterforskning. Er formålet å avklare om et straffbart forhold har funnet sted, er det etterforskning. Annen politivirksomhet, som forebyggende virksomhet og avdekking og stansing av mulige straffbare handlinger (etterretning), kan også innebære behov for informasjonsinnhenting. Slik informasjonsinnhenting har hjemmel i politiregisterloven.

Det er påtalemyndigheten som avgjør om etterforskning skal iverksettes. Beslutningen tas etter en vurdering av vilkårene i straffeprosessloven (strpl.) § 224. Etter straffeprosessloven § 225 er påtalemyndigheten ansvarlig for etterforskningen.

Skjer informasjonsinnhentingen i etterforskningssporet, gis ulike aktører i etterforskningen straffeprosessuelle rettigheter, eksempelvis rett til innsyn i sakens opplysninger etter strpl. § 242. Dersom informasjonsinnhentingen innebærer bruk av straffeprosessuelle tvangsmidler, må beslutning fra retten eller påtalemyndigheten innhentes.

Informasjonsinnhenting fra åpne kilder på internett er i utgangspunktet lovlig. Politiet må imidlertid ha en saklig grunn for informasjonsinnhentingen og den må være forholdsmessig. Grunnloven og EMK artikkel 8 setter yttergrenser for hvilke inngrep politiet kan gjøre. Hvorvidt en persons privatliv er vernet mot politiets informasjonsinnhenting, beror på en samlet vurdering av intensiteten i de konkrete tiltakene, og krever en konkret vurdering. Relevante vurderingstema kan være om informasjonsinnhentingen foregår over tid og gjennomføres systematisk, og om den finner sted på et privat område. Dersom innhentingsmåten griper inn i vernet etter EMK artikkel 8, må det aktuelle tiltaket, i tillegg til å være saklig begrunnet og forholdsmessig, ha hjemmel i lov. Uten slik hjemmel er tiltaket ulovlig.

Det er nødvendig at politiet har et bevisst forhold til informasjonsinnhenting fra åpne kilder på internett, og det er arbeidet med dette de senere år. Blant annet er *Personvernkommisjonen* kjent med at KRIPOS utarbeidet en nasjonal veileder på dette feltet i 2018.

Det er særlig viktig at politiet har høy bevissthet om personvernimplikasjonene knyttet til bruken av åpne kilder med henblikk på hvilke konsekvenser bruken kan ha for tilliten til politiet og for faren for nedkjølingseffekt i befolkningen.

Selv om det foreligger nødvendighets- og forholdsmessighetsvurderinger før informasjon innhentes, kan selve *muligheten* politiet har til å bruke opplysninger innhentet på nett til etterforskningsformål ha nedkjølingseffekter i form av at personer legger bånd på hva de gjør og sier i frykt for at dette kan få negative konsekvenser. Dette kan forekomme selv om man ikke faktisk er under overvåkning. Antagelsen eller fornemmelsen av at noen følger med kan være nok til å utløse effekten. Det kan således oppstå nedkjølingseffekter ved at politiet benytter opplysninger fra kommentarfelt eller sosiale medier. Det vil kunne være uheldig for ytringsfriheten dersom individer bevisst avstår fra å for eksempel ytre seg politisk i sosiale medier fordi de er bekymret for at ytringene kan tas ut av kontekst og/eller brukes på måter som i ytterste konsekvens kan få juridiske følger. Med nye, dynamiske metoder som stadig tas i bruk ved etterforskning av nettbasert kriminalitet, vil behovet for personvernkonsekvensvurderinger øke. Vurderingene bør brukes som et operativt verktøy i det daglige arbeidet med personvern for å samle flere miljøer og skape forståelse for ulike tiltak. I tillegg vil det kunne benyttes

for å identifisere praktiske, risikoreduserende tiltak, som er tilpasset miljøet disse tiltakene iverksettes i.

Personvernkommisjonen mener bruk av åpne kilder på internett kan skape særskilte personvernutfordringer. *Kommisjonen* er blant annet bekymret for hvilke nedkjølingseffekter som kan oppstå som følge av justissektorens bruk av åpne kilder på nett, og dette perspektivet må vektlegges ved utarbeidelse av interne instrukser og lignende.

Personvernkommisjonen mener at dersom det igangsettes tiltak som innebærer masseinnsamling av personopplysninger for nærmere angitte formål, er det viktig at metoder for dataseparasjon følges for å sikre at data kun benyttes til formål lovgiver har vurdert det nødvendig for.

7.4.2.3 Dataseparasjon

Dataseparasjon betyr at opplysninger lagres i adskilte databaser, enheter og områder for hvert formål og behandling. Ved å separere behandlinger og lagring av personopplysninger tilknyttet en enkeltperson, reduseres muligheten for å lage komplette profiler av hver enkelt registrerte. Separasjon er også en god måte å oppnå formålsbegrensning, samt urettmessig kobling og lenking mellom ulike datasett. Tabeller med personopplysninger bør ha kortere lagringstid med tidsfrist for automatisk sletting, mens tabeller uten personopplysninger kan lagres lengre. Tiltak for å oppnå dette kan være tilgangsstyring til tabeller, splitting av databasetabeller, skille mellom enheter med høy tillit og lav tillit, skille tilgang til områder i forhold til behov.[78]

7.4.2.4 Formålsutglidning i forbindelse med politiets myndighetsutøvelse

Med formålsutglidning menes en situasjon hvor personopplysninger som er innhentet til et bestemt formål senere benyttes til et annet, nytt formål. Slik utglidning kan skje gradvis gjennom praksis, for eksempel ved at flere personer enn tiltenkt registreres,[79] og at opplysningene, etter at de er registrert, blir tilgjengelig for flere formål enn opprinnelig planlagt.[80]

Formålsutglidning kan forekomme av ulike årsaker og på flere nivå i politiet. *Personvernkommisjonen* anser risikoen for slik utglidning som størst ved bruk av tiltak som ikke defineres som inngripende, da det for disse tiltakene foreligger færre interne og eksterne kontrollmekanismer, og avgjørelser i større grad kan gjøres på grunnlag av skjønnsmessige vurderinger.

Bruk av inngripende metoder, som skjulte tvangsmidler, er gjenstand for særskilte kontrollmekanismer. Kontrollsystemet består både av interne kontrollmekanismer som politiets- og påtalemyndighetens organinterne kontroll, og eksterne kontrollmekanismer som domstolskontroll og kontroll gjennom uavhengige utvalg og med advokatbistand. Dette kontrollsystemet har vokst frem som følge av uheldige erfaringer med politiets skjulte tvangsmiddelbruk.[81]

Personvernkommisjonen anser risikoen for formålsutglidning ved bruk av inngripende metoder som relativt lav, både som følge av det interne og eksterne kontrollregimet, og fordi domstolene legger til grunn et sterkt legalitetsprinsipp.

Den største risikoen for formålsutglidning i politiet, slik *Personvernkommisjonen* ser det, ligger på individnivå og i forbindelse med bruk av tiltak som (i dag) ikke defineres som inngripende for personvernet. Et eksempel på et slikt tiltak er bruk av opplysninger hentet fra åpne kilder på nett.

Formålsutglidning kan skje som følge av at hjemler er uklare og at vurderingene som den enkelte politiansatte må gjøre derfor åpner opp for stor grad av skjønn. Det kan også oppstå utilsiktet formålsutglidning som en følge av bredere samfunns- og kulturendringer, ved at grensene for hva som oppfattes som sensitivt eller inngripende endrer seg. For eksempel kan samfunnsforståelsen av hva som oppfattes som en religiøs ytring endre seg over tid. Slik kan opplysninger som tidligere var regnet som uproblematisk for politiet å behandle, bli gradvis mer utfordrende å behandle.

Tydelige hjemler er viktig for å hindre formålsutglidning. Videre er en sterk personvernkultur, kombinert med et robust internkontrollsystem, avgjørende for å forebygge slik utglidning. Notoritet – at det dokumenteres hvilke opplysninger som brukes til hva – er en viktig del av et slikt kontrollsystem. I tillegg til organisatoriske tiltak, herunder effektiv internkontroll, er tekniske tiltak viktig for å forebygge formålsutglidning. KRIPOS har gitt innspill til *Personvernkommisjonen* om at tilgangsstyringen i enkelte av saksbehandlingssystemene bør vurderes og tilgangsnivået bedre må tilpasses rollebaserte behov.

---

78 Datatilsynet. (2019). *Programvareutvikling med innebygd personvern*.

79 LB-2017-150679.

80 HR-2019-1226-A.

81 Bruce, I. & Haugland, G.S. (2014). *Skjulte tvangsmidler*. Universitetsforlaget, s. 117.

Personvernkommisjonen mener ledelsen i politiet må ha høy bevissthet om faren for formålsutglidning og at risikoen for slik utglidning må reduseres gjennom etablering av organisatoriske og tekniske tiltak. Et viktig tiltak i denne sammenheng er å bygge en god personvernkultur. Dette er et lederansvar.

7.4.2.5 Deling av opplysninger mellom politiet og andre myndigheter

Tydelige og forutsigbare rammer for informasjonsutveksling er en forutsetning både for godt personvern og for effektiv kriminalitetsbekjempelse. Politiet har i dag hjemler i eget lovverk som gir adgang til informasjonsdeling. Etter politiregisterloven § 30 har politiet adgang til å utlevere opplysninger innhentet til politimessige formål også til andre offentlige organer dersom det er i mottakerorganets interesse (til forvaltningsformål).

Politiet kan utlevere opplysninger til både offentlige og private aktører på nærmere bestemte vilkår, eksempelvis opplysninger om en arbeidstaker. For at opplysningene skal kunne brukes etter sin hensikt er det avgjørende at mottaker har et dekkende behandlingsgrunnlag for den videre behandlingen.

En utfordring oppstår der utleveringsadgangen betinges av en vurdering av mottakers interesse av opplysningene, jf. politiregisterloven §§ 30 og 31. Bestemmelsene hjemler utlevering til offentlige eller private mottakere, dersom det er nødvendig for å fremme mottakers oppgaver etter lov, eller for å hindre at mottakers virksomhet utøves på en uforsvarlig måte. Politiet må dermed vurdere relevansen av opplysningene opp mot mottakers regelverk. Dette er svært skjønnsmessige vurderinger og det kan være utfordrende å vurdere rekkevidden av hjemlene. Som følge av uklare hjemler eksisterer det en risiko for at opplysninger utleveres uten tilstrekkelig rettslig grunnlag, som igjen kan få store konsekvenser for den enkelte.

En annen utfordring knyttet til informasjonsutveksling mellom politiet og andre virksomheter i Norge er at politiet i noen sammenhenger har hjemmel til å utlevere opplysninger, men at mottaker ikke har behandlingsgrunnlag for å behandle de samme opplysningene. Dette gjelder for eksempel ved samarbeid med vekterbransjen. Dette samarbeidet er formalisert med en intensjonsavtale mellom Politidirektoratet og NHO Service og Handel, samt lokale avtaler. Politiet vil ofte kunne ha hjemmel til å utlevere opplysninger til sikkerhetsbransjen, for eksempel i politiregisterloven § 31, eller i politiregisterloven § 27 for å avverge eller forebygge kriminalitet. *Personvernkommisjonen* har hatt møte med bransjeforeningen NHO Service og Handel som organiserer en stor del av vekterbransjen. Fra NHO Service og Handel er det påpekt at vekterselskapene mangler selvstendig behandlingsgrunnlag for å behandle opplysninger som mottas fra politiet, noe som er et krav etter personvernforordningen artikkel 6. Det er formidlet til *Personvernkommisjonen* at bransjen ønsker en nærmere regulering av samarbeidet med politiet.

Forebygging er politiets primærstrategi[82] og politiet har egne hjemler for utlevering av opplysninger til forebygging, jf. politiregisterloven § 27 annet og fjerde ledd. Hvor langt politiet kan gå i sin forebyggende virksomhet følger ikke alltid like klart av regelverket, herunder hvilke forebyggende tiltak politiet kan iverksette overfor enkeltpersoner. Enkelte inngrep er hjemlet i politiloven kapittel II. Politiet kan for eksempel gripe inn for å stanse forstyrrelser av den alminnelige ro og orden, eller for å avverge lovbrudd, jf. politiloven § 7. For politiets forebyggende virksomhet utenfor politilovens inngrepshjemler kan det imidlertid være vanskeligere å trekke grensen mellom hva politiet kan og skal gjøre, og hva som for eksempel hører til andre etater, slik som skole, helsevesen eller barnevern. Dette kan medføre en utfordring med tanke på hvilke opplysninger om enkeltpersoner som kan behandles av hvem og til hvilke formål.

I politimeldingen, Meld. St. 29 (2019–2020) er det for eksempel lagt til grunn at politiet skal ta initiativ til lokale samarbeidsavtaler med kommunene, som blant annet bør omfatte tverrfaglig innsats for forebygging, samt at samarbeidet mellom politi, barnevern og skole skal styrkes.[83] Det er således en politisk forventning om samhandling og forebygging, uten at de rettslige rammene alltid er tilsvarende klare.

Et område der det for tiden pågår arbeid med hjemler og systemstøtte for samarbeid, er arbeidslivskriminalitetssamarbeidet (A-krimsamarbeidet) mellom politiet, Arbeidstilsynet, NAV og skattemyndighetene i A-krimsentrene. Justis- og beredskapsdepartementet arbeider med ny forskrift om deling av taushetsbelagte opplysninger

---

[82] Politidirektoratet. (2018). *Kriminalitetsforebygging som politiets primærstrategi 2018 – 2020: Politiet mot 2025 – delstrategi*.

[83] Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden*. Justis- og beredskapsdepartementet. Punkt 3.

og behandling av personopplysninger i det tverretatlige samarbeidet mot arbeidslivskriminalitet. I høringsrunden kom flere instanser med kritikk grunnet manglende personvernvurderinger. Datatilsynet pekte på at det er en betydelig mangel ved forslaget at det er ikke gjennomført nødvendige vurderinger av konsekvenser for de berørtes personvern og mente at forskriften ikke kunne vedtas slik den forelå. A-krimsamarbeidet er også diskutert i denne rapportens kapittel 6. Både politiet og de samarbeidende etatene har påpekt viktigheten av en bedre regulering av samarbeidet, og behovet for en avklaring av hjemmelsgrunnlaget for deling av opplysninger og hvem som skal være behandlingsansvarlig for de opplysningene som behandles i fellesskap.

Utfordringen med dagens regulering knytter seg til interesseavveininger som utleverende organ fortløpende må foreta, spesielt når utleveringen skjer til flere etater samtidig og hvor det foreligger ulike bestemmelser om taushetsplikt og behandling av opplysninger.

Samme type utfordringer kan også oppstå i andre tverretatlige samarbeid politiet deltar i. Andre eksempler på tverretatlig samarbeid er SaLTo-samarbeidet[84] mellom Oslo politidistrikt og Oslo kommune, og Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES).[85] Generelt kjennetegnes slike samarbeid av at det er politisk vilje og forventninger til tettere samhandling, men uten at regelverket nødvendigvis er oppdatert.

Personvernkommisjonen mener en klargjøring av hjemler og bevisstgjøring rundt personvernkonsekvenser av informasjonsdeling mellom etater og virksomheter er helt avgjørende for lovligheten av informasjonsdelingen.

7.4.3 Åpenhet om politiets metodebruk

Åpenhet bidrar til å skape tillit, og er en forutsetning for at innbyggerne skal kunne ivareta sine rettigheter og at det skal være mulig å kontrollere at regler etterleves. For å opprettholde prinsipper om åpenhet og etterrettelighet, må det eksistere mekanismer som gjør innbyggerne trygge på at myndighetene bruker sine virkemidler etter loven, og kun der det er foretatt grundige konsekvensutredninger.

Mangel på informasjon og gjennomsiktighet om teknologibruk, kombinert med en stadig utvikling av kraftige datainnsamlings- og analyseverktøy for bruk i justissektoren, kan føre til svakere personvern, men også til at befolkningens tillit til justissektoren svekkes. Dette kan over tid ha negative ringvirkninger som kan gjøre det vanskelig for justissektoren å utføre sine oppgaver.

Det er begrenset tilgjengelig informasjon om hvilke verktøy blant annet politiet i Norge anvender, og hvordan personvern ivaretas i praksis. Det er også *Personvernkommisjonens* erfaring at det i *kommisjonens* arbeid har vært utfordrende å få innsikt i metodebruk og verktøy som er i bruk eller som vurderes tatt i bruk. Dette gjenspeiler erfaringer gjort av Metodekontrollutvalget.

I 2009 la Metodekontrollutvalget frem sin evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker.[86] Utvalget pekte på metodologiske utfordringer i sin evaluering, blant annet knyttet til manglende registrering og statistikk over politiets tvangsmiddelbruk, samt taushetsbelagte saksdokumenter som begrenset muligheten til å kartlegge bruken og betydningen av inngripende metoder.[87] Det er grunn til å anta at politiets metodebruk har utviklet seg betydelig siden 2009, i tråd med både kriminalitetsutviklingen og teknologiske muligheter.

Bruken av private leverandører for personverninngripende teknologi i justissektoren kan skape grunnleggende utfordringer i tilfeller der det mangler åpenhet rundt anskaffelser og konsekvensutredninger. Utfordringene knyttet til politiets samarbeid med Palantir, som beskrevet i avsnitt 7.4.5, illustrerer dette. Det er derfor etter *Personvernkommisjonens* syn særlig viktig med åpenhet for å sikre forsvarlig bruk av IT-leverandører i justissektoren.

Personvernkommisjonen anbefaler at det nedsettes et utvalg for å utrede metodebruk i justissektoren. Utvalget bør vurdere personvernkonsekvenser av politiets metoder, særlig sett opp mot formålsprinsippet og proporsjonalitetsprinsippet. Dette arbeidet forutsetter at utvalget har tilgang på nødvendig informasjon om bruken av inngripende metoder og skjulte tvangsmidler. Dette er viktig både som et tillitsbevarende tiltak, og for å

---

84 SaLTo-modellen er en desentralisert samarbeidsmodell for Oslo politidistrikt og Oslo kommune om rus- og kriminalitetsforebyggende arbeid blant barn og unge. «SaLTo» står for «Sammen Lager vi et Trygt Oslo» og er Oslo sitt SLT-arbeid. Oslo kommune. (u.å.). *Forebygging av rus og kriminalitet*.

85 Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES) ble opprettet som et tiltak fra Regjeringen for å skjerpe politiets og kontrolletatenes innsats mot økonomisk kriminalitet, herunder arbeidslivsskriminalitet.

86 NOU 2003: 21 *Kriminalitetsbekjempelse og personvern – Politiets og påtalemyndighetens behandling av opplysninger*.

87 NOU 2003: 21 *Kriminalitetsbekjempelse og personvern - Politiets og påtalemyndighetens behandling av opplysninger*.

reise en åpen og demokratisk debatt om hvor grensen mellom personvern og kriminalitetsbekjempelse og forebygging bør gå.

7.4.4 Effektiv domstolskontroll

I avsnitt 7.2.3 beskrives viktigheten av domstolskontroll ved straffeprosessuelle tiltak av et visst alvor. *Personvernkommisjonen* har også fremhevet at det bør klargjøres i loven at alle som kan beslutte slike inngrep må vurdere om de samlede tiltak i den enkelte sak er forholdsmessige, og herunder skal den enkelte involvertes personvern vurderes.

En effektiv domstolskontroll forutsetter at lovbestemmelser med inngrepshjemler ikke gjøres for generelle av lovgiver. Jo mer konkret en lov er, dess bedre blir domstolen i stand til å utøve reell, rettslig kontroll.

I 2016 fremmet Justisdepartementet en proposisjon om endringer i straffeprosessloven. Det ble foreslått at politiet gis en utvidet adgang til å benytte skjulte tvangsmidler ved etterforskning, avverging og forebygging av alvorlige lovbrudd.[88] Dersom dette forslaget hadde blitt vedtatt, hadde domstolskontrollen blitt redusert til en vurdering av om tiltakene var formålstjenlige og saklig begrunnet. Etter kritikk ble lovendringen vedtatt med krav om at slike tiltak bare kunne iverksettes der det var objektive holdepunkter i selve saksforholdet som ga grunn til å undersøke om noen forbereder for eksempel en terrorhandling.[89] Gjennom denne endringen ble den reelle domstolskontrollen med PSTs virksomhet betydelig styrket, og rettssikkerheten til de involverte bedre ivaretatt.

Personvernkommisjonen mener det bør vurderes om dagens domstolskontroll av politiets tiltak bør utvides til å omfatte flere tiltak enn i dag. *Kommisjonen* understreker videre viktigheten av at bestemmelser som hjemler forskjellige tvangsmidler formuleres slik at effektiv og reell domstolskontroll blir mulig.

Etter straffeprosessloven § 170a kan et tvangsmiddel aldri brukes når det fremstår som et uforholdsmessig inngrep. Denne vurdering må alltid påtalemyndigheten og retten gjøre. Samtidig kan flere mindre inngripende tiltak ha en samlet effekt som utgjør et større inngrep i personvernet.

Som nevnt innledningsvis, reiser *Personvernkommisjonens* mandat spørsmål om det samlede omfang av tiltak innenfor justissektoren skaper utfordringer for personvernet. Denne problemstillingen er formentlig særlig adressert til etterforskning og de mulige metodene som i den sammenheng kan iverksettes, både av tradisjonell karakter (ransaking, pågripelse, beslag) og de mer ekstraordinære (kommunikasjonskontroll, hemmelig ransaking, romavlytting).

Kommisjonen understreker at det er ved den mest alvorlige kriminalitet spørsmålet om inngripende og omfattende tvangsmiddelbruk vil reise seg. De ulike metodene har gjerne blitt vedtatt over tid av lovgiver og skal og må stå i forhold til de utfordringer alvorlig kriminalitet til enhver tid utgjør. Kvalifiserte interesseavveininger er nødvendige; hvor alvorlig er det aktuelle inngrepet, vil iverksettelse av dette være hensiktsmessig med tanke på oppklaring og hvor alvorlig er den kriminalitet som begås?

Personvernkommisjonen mener det bør innføres et tillegg i straffeprosessloven § 170a som sikrer at det gjøres en vurdering av at den samlede bruken av ulike etterforskningsmetoder ikke blir et uforholdsmessig inngrep. I et slikt tillegg bør det understrekes at hensynet til personvern skal vektlegges i denne vurderingen.

7.4.5 Bruk av ny teknologi i justissektoren

Bruk av ny teknologi vil være svært viktig i justissektoren fremover, og kan bidra til mer effektiv kriminalitetsbekjempelse dersom den brukes på en forsvarlig måte. Feil eller ureflektert bruk av teknologi kan ha stor innvirkning på den enkeltes personvern og andre rettigheter og friheter. Ethvert tiltak må, som nevnt, tilpasses den kriminalitetstrusselen samfunnet står overfor, og faktiske situasjoner og hva som må til for å sikre innbyggerne mot kriminalitet forandrer seg stadig. Samtidig må det være en forutsetning at metodebruken er proporsjonal, og at den samsvarer med problemene man ønsker å løse.

Det er vanskelig å få en helhetlig oversikt over hvordan politiet i Norge benytter ny teknologi, som for eksempel maskinlæringssystemer. *Personvernkommisjonen* har imidlertid fått innspill fra professor Mareile Kaufmann fra Institutt for kriminologi ved Universitetet i Oslo om at det er mange ulike avdelinger innad i politiet som benytter forskjellige typer teknologier. Politiet ønsker, av hensyn til pågående og fremtidig etterforskning og kriminalitetsbekjempelse, ikke å avsløre nøyaktig hvilke metoder som benyttes.[90] Nasjo-

---

88 Prop. 68 L (2015–2016) *Endringer i straffeprosessloven mv. (skjulte tvangsmidler)*, kap. 13.4.

89 Prop. 68 L (2015–2016) *Endringer i straffeprosessloven mv. (skjulte tvangsmidler)*, kap.13.4.4.

nalt cyberkrimsenter (NC3) er det nasjonale senteret for forebygging, avdekking og bekjempelse av trusler og kriminalitet i det digitale rom.[91] Denne enheten kunne i 2020 meddele at de benytter maskinlæringssystemer til stordataanalyser. Per i dag benyttes ikke maskinlæringssystemer til formål som forutseende politiarbeid (se nedenfor) eller chatroboter. Stordataanalysene brukes imidlertid til å analysere store datamengder i etterforskningsarbeid.[92]

Nedenfor vil *Personvernkommisjonen* drøfte noen overordnede og prinsipielle personvernutfordringer som kan oppstå ved anskaffelse og bruk av ny teknologi i justissektoren. Flere av eksemplene er fra andre land, men det er nærliggende å tro at lignende problemstillinger kan oppstå dersom teknologien ønskes benyttet i norsk justissektor, selv om det juridiske og kulturelle bakteppet i mange tilfeller vil være annerledes.

7.4.5.1 Kommersielle analyseverktøy for bruk i justissektoren

Bruken av kommersielt utviklede overvåknings- og analyseverktøy i justissektoren har reist spørsmål både i Norge og i andre land. Det amerikanske analyse- og teknologiselskapet Palantirs samarbeid med myndigheter rundt om i verden kan tjene som eksempel. Selskapet leverer analyseverktøy til forsvar, etterretning og bedrifter verden rundt. På Palantirs kundeliste står blant annet CIA, FBI, NSA, og det amerikanske forsvaret, og selskapet leverer teknologi for alt fra DNA-sporing og børsanalyse til terrorbekjempelse og datadreven krigføring.[93]

I Norge inngikk Politidirektoratet i 2017 et samarbeid med Palantir, gjennom en bestilling av IKT-prosjektet Omnia.[94] Programvaren fra selskapet, som ble betegnet som «Google for politiet», skulle i utgangspunktet være et system for å utveksle opplysninger med politimyndigheter i andre land, som en del av det såkalte Prüm-samarbeidet[95] for etterforskning av grenseoverskridende saker. Verktøyet skulle også brukes til å sammenstille og analysere data fra politiets forskjellige registre, inkludert register om DNA, fingeravtrykk, etterforskningsopplysninger med mer, for å samle alt under ett system og finne nye sammenhenger som kunne brukes i pågående etterforskninger.

I 2020 ble det annonsert at prosjektet var ansett som avsluttet. Med en prislapp på over 100 millioner kroner var Omnia blitt implementert i en redusert versjon som saksbehandlingssystem med integrasjoner for Prüm-samarbeidet. Ved prosjektets avslutning var fortsatt flere av systemets kjernefunksjoner ikke-funksjonelle, og det var reist spørsmål om utvekslingen av personopplysninger i systemet var innenfor lovens grenser.[96] Tolletaten har også inngått et samarbeid med Palantir, med mål om at selskapets programvare vil bidra til mer effektivt og målrettet arbeid.[97]

Politiet i Danmark har også inngått samarbeid med Palantir, gjennom prosjektet POL-INTEL. Dette systemet gjør det mulig å sammenstille og analysere informasjon på tvers av politiets registre.[98] Før løsningen kunne tas i bruk, var det imidlertid nødvendig med en lovendring, da slik sammenstilling av opplysninger var på kant med blant annet prinsippene om dataminimering og formålsbestemthet i personvernforordningen. I 2017 ble en lovendring vedtatt. Loven gir dansk politi hjemmel til å foreta tverrgående informasjonsanalyser i politiets registre, samt å kunne samle og behandle opplysninger fra offentlig tilgjengelige kilder (inkludert å kjøpe personopplysninger fra datameglere),[99] dersom «det er nødvendig av hensyn til utførelsen av politiets oppgaver». Kritikere av lovendringen har påpekt at dette nærmest avskaffer formålsbegrensingsprinsippet for dansk politi, på bekostning av innbyggernes personvern.[100]

Det har blitt stilt en rekke spørsmål ved konsekvensene av at organer i justissektoren inngår samarbeid med kommersielle teknologiselskaper, fra blant annet pressen,[101] Datatilsynet,[102] akademikere[103] og politikere.[104] Kritikken har inkludert spørsmål om hvordan personvernhen-

---

90 Kaufmann, M. (2020). *Likestillingsombudets årskonferanse om kunstig intelligens i et likestillingsperspektiv*. (video).

91 Politiet. (u.å.). *Nasjonalt cyberkrimsenter (NC3)*.

92 Kaufmann, M. (2020). *Likestillingsombudets årskonferanse om kunstig intelligens i et likestillingsperspektiv*. (video).

93 The Guardian. (2017, 30. juli). *Palantir: the 'special ops' tech giant that wields as much real-world power as Google*.

94 Morgenbladet. (2021, 3. desember). *Slik ble politiets «supervåpen» en 100-millioners fiasko*.

95 Utenriksdepartementet (EU-delegasjonen). (2009, 23. mars). *Prüm forenkler DNA-sporing*.

96 Politiforum. (2020, 3. april). *Bråstopp for prestisjeprosjekt*.

97 Aftenposten. (2018, 23. januar). *Nå skal algoritmer og analyser av «big data» avgjøre hvem som blir sjekket ekstra nøye i tollen*.

98 Zetland. (2021, 4. mai). *For fire år siden fik politiet et «supervåben». Her er, hvordan det har transformeret ordensmagten*.

99 Se mer om datameglere i kapittel 9 om forbrukernes personvern.

100 Morgenbladet. (2021, 17. desember). *Overvåkning: Endret loven for å passe til Palantirs programvare*.

101 NRK Beta. (2021, 17. desember). *«Supervåpen» fra Silicon Valley ga hodebry og millionsprekk for politiet*.

102 Thon, B. E. (2018). *Algoritmene må temmes*. Aftenposten.

syn vurderes før og når teknologien anskaffes og tas i bruk, programvarens treffsikkerhet og formål, manglende åpenhet hos selskapene om systemene samt i de inngåtte avtalene, og at slike samarbeid kan skape uheldige avhengighetsforhold mellom justissektoren og store teknologiselskaper.

Personvernkommisjonen mener det er avgjørende med åpenhet og muligheter for kontroll ved anskaffelser i justissektoren. Ved anskaffelse av potensielt inngripende verktøy må personvernvurderinger være en sentral del av beslutningsgrunnlaget.

7.4.5.2 Utfordringer ved bruk av maskinlæringsmodeller i justissektoren

På grunn av informasjonsbehovet i justissektoren, kan bruk av maskinlæringssystemer og stordataanalyse være egnede verktøy.[105] Det utvikles en rekke verktøy som tar i bruk maskinlæring for å bidra til kriminalitetsbekjempelse og forebygging. Bruken av slike verktøy kan føre til mer effektiv ressursbruk, og kan for eksempel bidra til å redusere vilkårlighet og forskjellsbehandling. Gode verktøy kan også hjelpe politiet å utføre sitt samfunnsoppdrag på en bedre måte. Maskinlæringssystemer kan for eksempel benyttes til å profilere og organisere, se sammenhengen mellom ulike digitale identiteter som en gjerningsperson har brukt, flagge mistenkelig atferd på internett, eller søke etter utvalgte ord eller temaer i samtaler eller i kommentarfelt.

Som drøftet i kapittel 6, forutsetter ansvarlig bruk av maskinlæringssystemer at det gjennomføres gode forhåndsvurderinger og at det foreligger grundig dokumentasjon av systemene. Dersom teknologien ikke brukes riktig, innebærer det enkelte utfordringer, både ved bruk i politiet og i domstolsystemet. Disse vurderes kort nedenfor.

Som beskrevet i kapittel 5, kan maskinlæringssystemer ha alvorlige feilkilder som kan føre til uriktige resultater. Dette kan ha særlig alvorlige konsekvenser for enkeltindivider dersom systemene anvendes innenfor justissektoren.

Maskinlæringssystemer kan komme til unøyaktige resultater eller gjenskape diskriminerende mønstre som har satt seg i praksis over en lengre periode. Feil og systematiske skjevheter kan ha ulike kilder, som kan spores helt tilbake til hvilke treningsdata som var brukt ved utviklingen og testingen av systemet. Data som brukes i analysene gjenspeiler ikke nødvendigvis virkeligheten. Dersom algoritmer som er tenkt brukt i justissektoren trenes på data fra tidligere avsagte dommer kan de gjenta systematiske skjevheter fra tidligere praksis.[106] Data om kriminelle handlinger eksisterer kun dersom politiet oppdaget og registrerte handlingen, som betyr at det ofte er snakk om arrestasjonsdata i stedet for faktisk informasjon om kriminalitet. Dersom enkelte befolkningsgrupper eller geografiske områder oftere havner i politiets søkelys enn andre grupper, vil datagrunnlaget for systemene kunne føre til at beslutninger rammer skjevt og/eller diskriminerende.

Det kan også oppstå feil i utvelgelsen av variabler som danner grunnlaget for en avgjørelse. Når maskinlæringssystemet skal trenes, legger utvikleren som regel inn all informasjon man vurderer som relevant for systemets oppgaver. Det kan inkludere inntekt, hvor man bor, om man har kriminelle foreldre, og en lang rekke andre faktorer som kan vurderes som relevante. Dersom disse variablene overlapper med beskyttede kategorier, for eksempel ved at bosted korrelerer med etnisitet, kan konsekvensen i praksis bli som om man brukte etnisitet som en variabel i systemet.[107]

På justisområdet vil slike feil eller uheldige slutninger kunne ha svært alvorlige konsekvenser for den enkelte. Dette er også grunnen til at det nye forslaget til forordning for kunstig intelligens kvalifiserer anvendelse av denne typen teknologi til «rettshåndhevelse, migrasjon, asyl og grensekontroll, samt rettspleie og demokratiske prosesser», som høyrisiko, og dermed underlagt strenge forpliktelser før løsningene slippes ut på markedet.[108] Forslaget til forordning for kunstig intelligens omtales nærmere i kapittel 9 om forbrukernes personvern.

Som beskrevet i kapittel 5, kan det være vanskelig å forstå hvordan et maskinlæringssystem har kommet frem til en bestemt avgjørelse. Manglende transparens kan føre til at systemene blir en «svart boks», som gjør at det kan være svært vanskelig for sakens parter å bestride avgjørelsen. Dersom teknologien er utviklet av et privat sel-

[103] Politiforum (2018, 8. april). *Selv om en salgsbrosjyre sier at et dataverktøy kan tenke som et menneske, bør man ikke stole på det.*

[104] NRK. (2018, 24. april). *Må svare om kontrakter med selskap knyttet til Facebook-skandalen.*

[105] UNICRI. (2019). *Artificial intelligence and robotics for law enforcement.*

[106] NOU 2020: 11 *Den tredje statsmakt – Domstolene i endring,* s. 258.

[107] Goodwin, M. (2020). *AI – myten om maskinene.* Humanist Forlag, s. 107.

[108] Stortinget. (2021, 23. april). *Historisk EU-regulering av kunstig intelligens (AI).*

Boks 7.3 Bruk av forutseende teknologi av Chicago-politiet

I 2012 innførte Chicago-politiet et maskinlæringssystem for å tildele personer som var blitt arrestert en trussel-score fra 1 til 500. Scoren skulle blant annet hjelpe politiet å beslutte om personen skulle få hjemmebesøk etter løslatelsen, om det skulle igangsettes ekstra overvåking av vedkommende, og gi politiet en indikasjon på om personen utgjorde en mulig trussel.[1] Dette skulle bidra til målretting av tiltak fra politiets side og redusert risiko ved anholdelser.

Etter åtte år ble programmet skrinlagt da nytteverdien hadde vært marginal, og systemet ikke hadde bidratt til mindre kriminalitet. Videre viste det seg at algoritmen, som benyttet treningsdata fra tidligere saker og straffedømte, ikke tilstrekkelig vektla hvorvidt arrestasjonen førte til domfellelse, og som innebar at systemet ga liten indikasjon på hvorvidt individet faktisk hadde begått en kriminell handling. Algoritmen virket diskriminerende ved å utsette de som ble gitt høy trussel-scoring for ytterligere kontrolltiltak.

Manglende gjennomsiktighet skapte dessuten frykt og mistillit mot programmet, som faktisk var til hinder for politiets forebyggende arbeid. Politiet fikk heller ikke tilstrekkelig opplæring i bruken av systemet og hadde dermed ikke forutsetninger til å anvende det på en effektiv måte. Politiet delte også data med andre offentlige myndigheter, uten å gi mottakere nødvendige forklaringer på hvordan informasjonen skulle leses og brukes.[2]

Kritikere av bruken av slike maskinlæringssystemer i justissektoren har pekt på at slike tiltak setter uskyldige under mistanke, at det kan sette søkelys på individer som ikke er under mistanke og at politiets intervensjon kan bli en selvoppfyllende profeti, ved at personer som behandles som mulige kriminelle kan ende opp på feil side av loven.[3]

[1] Ferguson, A. G. (2017, 3. oktober). *The police are using computer algorithms to tell if you're a threat.* Time.

[2] Chicago Tribune. (2020, 25. january). *For years Chicago police rated the risk of tens of thousands being caught up in violence. That controversial effort has quietly been ended.*

[3] The Verge. (2021, 24. mai). *Heat Listed.*

skap, er det ikke uvanlig at systemets interne logikk hemmeligholdes som en forretningshemmelighet.

Det kan også oppstå utfordringer dersom maskinlæringssystemer som forutser risiko benyttes som beslutningsstøtte i justissektoren. Ved å analysere store mengder informasjon om befolkningen, kan det utledes risiko for at et individ for eksempel vil komme i kontakt med kriminelle miljøer, utføre kriminelle handlinger, eller få tilbakefall ved prøveløslatelse. I tilfeller der slike systemer brukes til beslutningsstøtte uten at nødvendige risikovurderinger er gjort i forkant, kan individer settes under mistanke på grunn av antatte fremtidige handlinger basert på statistikk og informasjon om store deler av befolkningen. Som beskrevet i kapittel 6, kan det være vanskelig eller umulig for saksbehandlere å overprøve anbefalinger fra maskinlæringssystemer dersom nødvendige forbehold ikke er tatt. Dersom beslutninger tas basert på kompliserte statistiske modeller som er vanskelig å forklare eller forstå, kan det skape grunnleggende utfordringer for rettssikkerheten ved at det blir vanskelig å forklare hvorfor man har landet på den konkrete beslutningen.

Personvernkommisjonen er bekymret for feil bruk av maskinlæringssystemer i justissektoren. Beslutninger som ikke kan etterprøves eller fører til at store mengder opplysninger om den enkelte innbygger samles inn og behandles, vil i ytterste konsekvens kunne føre til nedkjølingseffekter og svekket ytringsfrihet, bevegelsesfrihet og rettssikkerhet.

Personvernkommisjonen mener det bør tas spesielt hensyn til etterprøvbarhet og ivaretagelse av den enkeltes rettigheter ved bruk av maskinlæringssystemer i justissektoren. For at slike metoder skal kunne tas i bruk i Norge, må de også være forklarbare for den som anvender teknologien, og risikovurderinger og pålagt teknisk dokumentasjon må foreligge i tråd med forslaget om forordning for kunstig intelligens.[109]

7.4.5.3 Utfordringer ved bruk av store datamengder

Muligheten for å analysere og anvende store informasjonsmengder (stordataanalyse) kan være

[109] Forslag til forordning for kunstig intelligens, Artikkel 11 og Annex IV EUR-Lex – 52021PC0206 – EN – EUR-Lex.

Boks 7.4 Seriemorder avslørt av kommersiell DNA-test

I 2018 arresterte politiet i Los Angeles seriemorderen kjent som The Golden State Killer ved bruk av kommersiell gentesting. Etterforskerne sendte DNA-funn til to forbrukerrettede gentestingselskaper, og fikk treff på en slektning av gjerningsmannen, som hadde tatt en selvtest hos det samme selskapet.[1] Arrestasjonen skapte oppmerksomhet i USA rundt justissektorens tilgang på og bruk av kommersielle DNA-databaser.

[1] Los Angeles Times. (2020, 8. desember). *The untold story of how the Golden State Killer was found: A covert operation and private DNA.*

et nyttig verktøy for politiet. Det kan for eksempel bidra til å identifisere personer som har beveget seg i nærheten av et åsted eller finne personer som er etterlyste. Samtidig reiser bruken av store mengder data for å gjennomføre analyser i justissektoren noen prinsipielle spørsmål om hvor grensen går mellom kriminalitetsforebyggende hensyn og retten til personvern.

Stordataanalyse vil i mange tilfeller forutsette at personopplysninger om store befolkningsgrupper behandles for å finne mønstre som kan identifisere mistenkte eller annen relevant informasjon i en pågående sak. I slike tilfeller vil et stort antall individer som ikke har noe med saken å gjøre indirekte kunne havne i politiets søkelys.

For eksempel utreder politiet i Norge mulighetene for bruk av DNA-analyser ved hjelp av kommersielle slektskapsdatabaser. Denne utviklingen har blitt kritisert av Datatilsynet på grunn av overvåkningspotensialet ved bruk av kommersielle databaser, da det innebærer behandling av personopplysninger om individer utenfor mistanke.[110] I 2020 ble det svenske politiet bøtelagt av det svenske datatilsynet for å ha anvendt kommersielle slektskapsdatabaser i etterforskningen av en drapssak uten å ha gjennomført nødvendige personvernvurderinger.

Som beskrevet i kapittel 5, er bruk av ansiktsgjenkjenning og lignende verktøy for biometrisk fjernidentifisering særlig inngripende for personvernet, da det innebærer registrering av en stor mengde individer som ikke er under mistanke.

[110] Bioteknologirådet (2021, 20. oktober). *Datatilsynet vil ha klare begrensninger på politiets bruk av DNA.*

Boks 7.5 Svensk politi brukte kontroversielt ansiktsgjenkjennings-verktøy

I 2021 avslørte nettstedet Buzzfeed at politiet i minst 24 land hadde tatt i bruk ansiktsgjenkjenningsteknologi fra det omstridte selskapet Clearview AI.[1] Verktøyet bruker maskinlæring for å sammenligne ansikter med bilder i en database som inneholder over tre milliarder bilder hentet fra sosiale medier og andre åpne kilder. I følge Buzzfeed har ansatte i politiet i flere land brukt systemet i forsøk på å identifisere gjerningspersoner, i mange tilfeller uten tillatelse fra sine overordnede. I Sverige utstedte det svenske datatilsynet en bot til politiet for bruken av Clearview, fordi de hadde behandlet biometriske data uten gyldig behandlingsgrunnlag og uten å gjennomføre en personvernkonsekvensvurdering.[2] Teknologien har i følge Buzzfeed ikke blitt brukt av norsk politi.

[1] BuzzFeed. (2021, 25. august). *Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here.*

[2] Integritetsskyddmyndigheten. (2021, 2. oktober). *Beslut efter tillsyn enligt brottsdatalagen – Polismyndighetens användning av Clearview AI.*

Dersom kameraer som bruker ansiktsgjenkjenningsteknologi plasseres i offentlig rom for å identifisere mistenkte individer, vil nødvendigvis biometriske data registreres om samtlige personer som fanges opp av kameraet. I motsetning til tidligere bruk av kameraovervåkning, forutsetter ikke ansiktsgjenkjenningssystemer at en etterforsker må gjennomgå materialet manuelt for å registrere individer av interesse – samtlige personer som fanges opp av kameraet registreres automatisk i sanntid. Dette legger press på personvernet til individer som i utgangspunktet ikke er i politiets søkelys. Det kan også oppstå problemer dersom systemet identifiserer feil person. Erfaringer fra andre land viser at enkelte ansiktsgjenkjenningssystemer har lavere treffsikkerhet i å korrekt identifisere individer fra enkelte etnisiteter eller grupper sammenlignet med andre etnisiteter og grupper, noe som kan få alvorlige følger dersom uskyldige blir feilaktig identifisert.[111]

[111] The National Institute of Standards and Technology. (2019). *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software.*

Personvernkommisjonen anbefaler et generelt forbud mot bruk av ansiktsgjenkjenning og annen biometrisk fjernidentifikasjon i offentlige rom. Et slikt forbud vil åpenbart begrense mulighetene for oppklaring av enkelte former for kriminalitet, men etter *kommisjonens* syn er teknologien såpass inngripende at den vanskelig kan forenes med grunnleggende rettigheter og samfunnsverdier.

Muligheten for og ønsker om masseinnsamling av data som en del av kriminalitetsbekjempelse kan også føre til at individer som ikke ønsker å spores eller registreres på nett, mistenkeliggjøres. Teknologi for å kommunisere fritt og sikkert via internett er et viktig verktøy for å ivareta grunnleggende rettigheter som ytringsfrihet og personvern. For eksempel er ende-til-ende-kryptering et verktøy som gjør at kommunikasjon ikke kan fanges opp og leses av uvedkommende. Enkelte myndigheter har uttrykt ønske om å forhindre eller forby bruk av ende-til-ende-kryptering, fordi teknologien kan gjøre det vanskeligere å avdekke kriminelle nettverk.[112] Slike lovforslag har blitt møtt med motstand og argumenter om at kryptert kommunikasjon blant annet er et nødvendig verktøy for journalister,[113] aktivister, varslere, utsatte grupper i konfliktsoner[114] og generelt for innbyggere som ønsker å kommunisere privat og sikkert.

Personvernkommisjonen mener det er viktig at politiet settes i stand til å håndtere alvorlig kriminalitet, men dette bør skje med minst mulig inngrep i mulighetene for fri og sikker kommunikasjon. Mistankekrav og krav om klar og tydelig lovhjemmel og domstolskontroll ved inngrep må ligge fast.

7.4.6 Personvernkompetanse

Når nye digitale verktøy og metoder vurderes tatt i bruk som ledd i myndighetsutøvelsen i justissektoren, er det et lederansvar å sørge for at ansatte har tilstrekkelig personvernkompetanse og at det finnes gode rutiner, som sørger for at personvernet til de som berøres av verktøyene og metodene ivaretas. Det er også et lederansvar å påse at virksomheten har tilstrekkelig personvernkompetanse til å foreta grundige personvernvurderinger i forbindelse med både lovarbeid og anskaffelse og bruk av verktøy som kan gripe inn i personvernet til innbyggerne. I 2021 ble det, som beskrevet i avsnitt 7.4.5, avslørt at enkelte tjenestepersoner i svensk politi hadde valgt å ta i bruk det inngripende ansiktsgjenkjenningsverktøyet Clearview AI, uten at dette var forankret i organisasjonen. Dette illustrerer viktigheten av gode rutiner, opplæring og etablering av robuste kontrollrutiner som kan avdekke avvik og kontroller at rutiner følges.

Personvernkommisjonen kan ikke se at politiet i tilstrekkelig grad har vektlagt å øke medarbeidernes bevissthet rundt personvern. Personvernkompetanse og -kultur må forankres i ledelsen i politiet. Det må også vies ressurser til at personvernombud kan legge til rette for kompetanseheving i organisasjonen.

Etablering av en god personvernkultur er en forutsetning for systematisk, varig og god ivaretakelse av personvernet. Det innebærer en grunnleggende forståelse og oppfatning i organisasjonen av at personvern er en verdi i seg selv, ikke en bremsekloss som kommer i veien for utførelsen av andre oppgaver. Personvernkulturen må være

Boks 7.6 Automatisk bildegjenkjenning på mobiltelefoner

I 2021 kunngjorde Apple at de ville rulle ut en ny teknologi på flere iPhone-modeller som skulle bidra til å avdekke overgrepsmateriale mot barn.[1] Teknologien fungerer ved at kjente overgrepsbilder gis en unik kode («hash»), og at bilder som er lagret lokalt på en telefon gis tilsvarende koder. Kodene sammenlignes, og dersom systemet finner en match flagges det til relevante myndigheter. Det betyr at overgrepsmateriale kan identifiseres selv om det ikke har blitt lastet opp på nett. Kunngjøringen ble møtt med motstand. Blant annet advarte kritikere mot faren for formålsutglidning ved at teknologien kunne utvides til å lete etter andre typer materiale. For eksempel kan teknologien tenkes brukt til å finne politiske dissidenter.[2] På grunn av kritikken har Apple utsatt utrullingen av teknologien på ubestemt tid.

1 The Verge. (2021, 15. desember). *Apple scrubs controversial CSAM detection feature from webpage but says plans haven't changed.*

2 The Register. (2021, 16. desember). *Apple quietly deletes details of derided CSAM scanning tech from its Child Safety page without explanation.*

112 TechCrunch. (2020, 9. desember). *On encryption and counter-terrorism, EU lawmakers say they'll work for 'lawful' data access.*

113 Press Freedom Institute. (2021, 21. oktober). *Global Encryption Day: Secure communication vital for journalists.*

114 The Washington Post. (2022, 8. mars). *Why encryption can be a matter of 'life or death' in Russia, Ukraine.*

forankret på ledelsesnivå for å bli en integrert del av organisasjonen.

Kripos har gitt innspill til *kommisjonen* om at bevisstheten om personvern er økende i politiet. Kripos har bygget et personvernfaglig miljø som de anser positivt for både etatens etterlevelse av regelverket, personvernet til de registrerte, samt for en effektiv kriminalitetsbekjempelse. I følge Kripos er det imidlertid store forskjeller på personvernkompetansen i enhetene i politiet.

Etter samtaler med aktører i justissektoren er det *Personvernkommisjonens* inntrykk at personvernvurderinger og interesseavveininger ofte overlates til den enkelte ansatte ved behandling av konkrete saker. Dette kan skape utfordringer for personvernet, for eksempel ved at mangelfulle vurderinger fører til uforholdsmessig eller vilkårlig praksis.

Politidirektoratet er behandlingsansvarlig for politiets sentrale behandlinger av personopplysninger etter personopplysningsloven. På politiregisterlovens område er det for de fleste av de sentrale registrene angitt i politiregisterforskriften at det er Kripos som er behandlingsansvarlig.

Kripos har videre det overordnede fagansvaret for personvern i politiet og ivaretar dette ansvaret ved generell opplæring, utarbeidelse av skjemaer, maler og sjekklister for vurderinger av personvernkonsekvenser. Gjennom kompetansetiltak rettet mot personvernombud og personvernrådgivere legger Kripos til rette for at kompetansekrav på personvernområdet er definert og blir innarbeidet enhetlig i de ulike politidistriktene.

Kripos er behandlingsansvarlig, men oppfølgingen av ansvaret er delegert nedover i styringslinjen. Det synes ikke å være tilstrekkelig avklart hvilke vurderinger som skal gjøres sentralt og hvilke som skal gjøres lokalt. Dette kan henge sammen med mangelfulle internkontrollrutiner eller mangelfull implementering av rutinen, eller med utydelige roller og ansvar. Kripos har uttrykt til *kommisjonen* at det er ønskelig med 100 % dedikerte personvernressurser i politidistriktene. Økt kompetanse og økt bevissthet vil gjøre tjenestepersoner mer rustet til å foreta flere av vurderingene selv, og velge personvernvennlige fremgangsmåter.

Personvernkommisjonen mener tjenestepersoner i politiet bør ha grundigere opplæring i personvern enn det som i dag er tilfellet. Behovet er spesielt stort i forbindelse med bruk av IKT-systemer i det daglige politiarbeidet, ved vurdering av personvernkonsekvenser ved innhenting og utlevering av personopplysninger, og ved samarbeid med andre offentlige eller private virksomheter.

Politidistriktene har opprettet enheter for digitalt politiarbeid (DPA), som bistår i etterforskningen av IKT-kriminalitet, og i sikring og analyse av elektroniske spor. I tillegg til særorganer som Kripos og Økokrim, har disse enhetene en avgjørende rolle, ikke bare i etterforskningen av IKT-kriminalitet, men også i etterforskningen av øvrige saker der det innhentes og behandles digitale spor.

Personvernkommisjonen mener personvernkompetansen i enhetene for digitalt politiarbeid (DPA) i politidistriktene bør styrkes, slik at alle operative beslutninger knyttet til elektronisk behandling av personopplysninger foregår innenfor eksisterende rettslige rammer for personvern, og etter robuste risikovurderinger. DPA-enhetenes samarbeid med personvernrådgivere og personvernombud i politiet må avklares og innarbeides mer enhetlig, gjerne gjennom nasjonale retningslinjer.

Personvernkommisjonen har fått innspill om at det ikke er opplæring om politiregisterloven eller personvernregelverket i politiutdanningen. *Personvernkommisjonen* mener dette er svært uheldig, da politiet jevnlig må forholde seg til registrene og bør ha kunnskap om regelverket. Mangel på personvernkompetanse og kunnskap om regelverket kan føre til formålsutglidning, ved at personopplysninger benyttes uten faktisk rettslig grunnlag. Dette kan også føre til at den enkelte blant annet ikke har mulighet til å ivareta sine rettigheter og ikke blir informert tilstrekkelig. En annen konsekvens er at tilliten til politiet kan svekkes.

Ved Politihøgskolen undervises det i etikkfag i alle årene i den treårige utdannelsen. Det første studieåret må studentene gjennom faget «Politi, samfunn og etikk» hvor ett av læringsmålene er at studenten skal ha «kjennskap til teknologisk utvikling og digitaliseringens muligheter og utfordringer».[115] Utover dette ser det ikke ut til at personvern er en egen del av utdanningsprogrammet.

Personvernkommisjonen mener undervisningen i personvern ved Politihøgskolen må styrkes. Politihøgskolen har en viktig oppgave i å bygge opp forståelse allerede i utdanningsløpet for viktigheten av personvern i politiets daglige arbeid. Dette vil bidra til å heve bevisstheten om person-

[115] Programplan bachelor – politiutdanning 2020-2023 (politihogskolen.no).

vern i politiet og bygge en sterkere kultur for vektlegging av personvernhensyn.

7.4.7 Systemer og verktøy for å ivareta personvernet

I tillegg til klare lovhjemler, tydelige ansvarsforhold og kompetanse, er gode informasjonssystemer og god infrastruktur en forutsetning for godt personvern. Manglende opplysnings- og systemkvalitet vil kunne gi en rekke uønskede konsekvenser. Innen justissektoren vil slike feil kunne få svært alvorlige konsekvenser for den enkelte, for eksempel urettmessig strafferettslig forfølgning.

Personvernkommisjonen har mottatt innspill fra politiet om at det er personvernutfordringer knyttet til bruk av politiets interne systemer. Blant annet oppstår det problemer ved saksbehandlings- og arkiveringssystemet Websak, som i følge Kripos skaper utfordringer med å ivareta personvernet ved utveksling av informasjon. Systemet har også skapt utfordringer ved bruk av tilgangskontroll og skjerming av materiale.

Personvernkommisjonen peker på at det er avgjørende at politiet har interne systemer som er utformet for å gjøre saksbehandlere i stand til å ivareta personvernet.

I det følgende vil *Personvernkommisjonen* trekke frem noen eksempler på systemer og verktøy som ikke ivaretar hensynet til personvern i tilstrekkelig. Det gjelder personvernutfordringer i forbindelse med digitale beslag og ved utveksling av dokumenter i justissektoren.

7.4.7.1 Håndtering av digitale beslag og overskuddsinformasjon

Riksrevisjonen avdekket i sin undersøkelse at politiet mangler en tilfredsstillende infrastruktur for håndtering av digitale beslag. Det digitale lagringsnettet (Digitale spor og beslag – DSB-nettet), som er tatt i bruk i alle politidistrikt med unntak av Oslo Politidistrikt, dekker ikke fult ut politiets behov for deling og lagring av elektronisk bevismateriale.

Personvernkommisjonen har gjennom dialog med nøkkelpersoner i politiet også fått opplyst at manglende mulighet til å filtrere bort overskuddsinformasjon ved beslag av digitale lagringsenheter, utgjør en særlig risiko for de registrertes personvern.[116] Når politiet beslaglegger en digital enhet, som for eksempel en datamaskin eller en mobiltelefon, vil det ofte også følge med informasjon som ikke er relevant for saken. Det finnes i dag ikke tekniske muligheter/verktøy for å filtrere bort slik overskuddsinformasjon. Det finnes heller ikke en spesialisert enhet[117] som har myndighet til å gjennomgå og filtrere bort åpenbart irrelevante personopplysninger. Konsekvensen av at det per i dag ikke foreligger tekniske muligheter til å filtrere ut overskuddsinformasjon, eller en spesialisert enhet som har som oppgave å trekke ut informasjon uten betydning, er at mengder av personopplysninger som ikke er relevant for saken blir tatt vare på, og gjort tilgjengelig for mange.

Et tungtveiende argument for å begrense adgangen til bruk av overskuddsinformasjon er at bruk av slikt materiale, i tillegg til å berøre personvernet til den som er involvert i saken, også ofte vil utgjøre et inngrep overfor andre personer som informasjonen omhandler, og som ikke nødvendigvis har gjort noe straffbart. Hensynet til utenforstående tredjepersoner taler for at bruken av overskuddsinformasjon bør begrenses.

I desember 2020 ble Norge dømt i den Europeiske menneskerettsdomstolen for krenkelse av EMK artikkel 8, i forbindelse med beslaget av mobiltelefonen til en siktet.[118] Etter straffeprosessloven § 119 har politiet ikke adgang til å ta beslag i korrespondanse mellom siktede og forsvareren, og i denne konkrete saken påberopte siktede seg at det fantes slikt materiale på telefonen. For å finne ut hva som er advokatkontakt, må noen se gjennom materialet. Kjernen i problemet er *hvem* som skal gjøre utsorteringen av materiale som er underlagt beslagsforbud. Norge ble derfor dømt for å ikke ha en prosess for utfiltrering av informasjon omfattet av yrkesmessig taushetsplikt ved beslag av digitale enheter. EMD mente det rettslige rammeverket rundt prosessen med utsortering var for uklart, og at Norge derfor ikke i tilstrekkelig grad beskyttet den beslagsfrie advokatkorrespondansen.

Avgjørelsen fra EMD medfører at norsk påtalemyndighet nå har plikt til å sortere ut materiale som kan være omfattet av beslagsforbud, og

---

[116] Begrepet «overskuddsinformasjon» i personvernretten benyttes for all informasjon som etter formålsbegrensningsprinsippet ikke er nødvendig for å oppnå formålet opplysningene er innhentet for. Dette kan være opplysninger om en annen person enn behandlingen gjelder, informasjon om forhold som er uten relasjon til selve formålet eller informasjon som ikke bidrar til å oppnå formålet med behandlingen. Overskuddsinformasjon trenger med andre ord ikke nødvendigvis å dreie seg om andre straffbare forhold.

[117] Rett24. (2021, 3. januar). *Riksadvokaten beordrer brems i politiets mobilgjennom.*

[118] Saber v. Norway [J], no. 459/18, (2020), ECHR:2020:1217.

levere dette tilbake uten nærmere gjennomsyn. Materiale som det kan reises spørsmål om er undergitt beslagsforbud, skal usett overleveres til tingretten for gjennomgang.

Ved et direktiv fra riksadvokaten i juni 2021 ble det innført et system der en egen teknisk enhet, organisatorisk atskilt fra etterforskningsenheten, har ansvar for å gjennomgå digitale enheter i forbindelse med beslag. Ordningen skal hindre at etterforskere får innsyn i opplysninger som det er forbudt å beslaglegge.

Personvernkommisjonen har blitt gjort oppmerksom på at det i enkelte europeiske politisystem finnes ordninger som setter skranker for politiets tilgang til all informasjon i en etterforskning, og ikke bare den som ikke kan beslaglegges. Det dreier seg om egne tekniske enheter i politiet som går gjennom for eksempel den beslaglagte informasjonen fra den aktuelle smarttelefon og deretter gir etterforskerne tilgang til det de mener er relevante opplysninger, basert på en bestilling fra dem som etterforsker den konkrete saken. Politibetjentene i de tekniske enhetene er ikke involvert i etterforskningen.

Personvernkommisjonen mener norske myndigheter bør innhente erfaringer fra andre land om ordninger for å filtrere bort overskuddsinformasjon ved beslag av digitale lagringsenheter og vurdere å etablere en lignende ordning. Personvernhensyn må alltid veies opp mot hensynet til oppklaring av kriminalitet der man i en dynamisk etterforskning ikke alltid i starten har full oversikt over hva slags informasjon som senere kan vise seg å få betydning som bevis.

7.4.7.2 Utlevering av dokumenter til advokater

Det kan oppstå personvernutfordringer ved bruk av enkelte av dagens systemer for utveksling av dokumenter i justissektoren, blant annet ved overføring av straffesaksdokumenter til advokater. *Personvernkommisjonen* har hatt dialog med representanter fra politiet og Advokatforeningen, som belyser at reglene om dokumentutlevering praktiseres ulikt mellom politidistrikter. Både politiet og Advokatforeningen vurderer dagens ordning for dokumentkopier og utlån som uhensiktsmessig og ressurskrevende, og risikoen for spredning av personopplysninger fremstår som stor.

Selv om utsendelse av dokumenter til forsvarere og til domstol i stor grad skjer via Altinn, har politiet opplyst til *Personvernkommisjonen* at det oppleves at det er lite kontroll med bruk av kopier etter at de er kommet frem til mottakere. Utlevering av dokumentkopier foregår i utstrakt grad, noe som innebærer en stor risiko for at informasjon kommer på avveie. Når det gjelder store mengder data som advokater har saksinnsyn i, utleveres disse på krypterte lagringsenheter. I flere tilfeller kopieres data deretter over fra lagringsenheten til andre lagringsmåter som ikke nødvendigvis ivaretar krav til informasjonssikkerhet ved oppbevaring av særlige kategorier av personopplysninger.

Politiet erfarer også at det kan være utfordrende å få tilbakelevert dokumenter fra advokater. Dette gjelder særlig ved advokat/forsvarerbytte. Dette kan også føre til at personopplysninger kommer på avveie. For eksempel kan informasjon som er slettet hos politiet dukke opp i forbindelse med en annen sak, som følge av lav bevissthet og kontroll på sletting og gjenbruk av opplysningene hos advokatene. Kripos opplyser også at det er noe uklart hvilke regler som gjelder for forsvareres videre oppbevaring av dokumentene, og praksis kan synes å variere også her. *Personvernkommisjonen* har fått opplyst at Tilsynsrådet for Advokatvirksomhet har intensivert kontroll med advokatenes behandling av utlevert materiale. Dette er en positiv utvikling og noe som definitivt er med på å redusere risikoen, men det er fortsatt et behov for bedre tekniske løsninger for utlevering og oppbevaring.

Utfordringene ved at personopplysninger kommer på avveie, samt størrelsen på filene det gis tilgang til, tilsier at elektronisk tilgang via en plattformløsning med sikkert grensesnitt og uten nedlastningsmuligheter vil gi bedre kontroll på utlevering av personopplysninger enn dagens ordning via Altinn. En mulig slik løsning er nærmere beskrevet i Kripos sin høringsuttalelse til Metodekontrollutvalgets rapport.[119] Domstolene forval-

[119] Kripos skriver følgende i sitt høringssvar til NOU 2009: 15 *Skjult informasjon – åpen kontroll. Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker*. Justis- og politidepartementet. «Kripos foreslår videre at det tas initiativ til å utrede en ordning med innsyn via sikker datalinje (VPN-løsning) til en server hos Seksjon for nasjonal KK ved Kripos. Denne seksjonen forvalter det nasjonale ansvaret Kripos har for kommunikasjonskontroll, og etterforsker ikke egne saker. Enheten er hovedsakelig bemannet med ingeniører. Ved denne formen for innsyn vil mistenkte og hans forsvarer ha mulighet til å se et speilbilde av kommunikasjonen via en sikker internettlinje fra en vanlig PC. Informasjonen kan ikke kopieres og aktiviteten kan loggføres. Tilgangen til informasjon og system kan kontrolleres fra politiets system, og kontrollutvalget for kommunikasjonskontroll kan føre kontroll med politiets håndtering av systemet. Det må understrekes at en slik løsning forutsetter at norsk politi går over til et sentralisert system for kommunikasjonskontroll. Planer for en slik løsning er for tiden til vurdering hos Politidirektoratet.»

ter også en aktørportal hvor advokater kan utveksle informasjon med domstolene.[120]

Personvernkommisjonen har ikke hatt kapasitet til å undersøke systemer for dokumentutveksling i forvaltningen av sivile saker, men det er grunn til å tro at disse systemene kan ha lignende svakheter knyttet til tilgangskontroll, gjenbruk og ulik praksis. I tillegg til et behov for bedre systemer for utlevering av dokumenter, er det også utslagsgivende at mottaker av dokumenter har egne systemer som også ivaretar sikkerheten og personvernet.

Personvernkommisjonen mener Justis- og beredskapsdepartementet bør etablere en samhandlingsplattform for dokumentutlevering i justissektoren. Plattformen bør utvikles med personvern og sikkerhet for øye, og bør blant annet ha funksjoner for å begrense muligheter for nedlasting og loggingsfunksjoner for å begrense urettmessig gjenbruk av dokumenter.

Personvernkommisjonen mener Justis- og beredskapsdepartementet bør etablere en norm for IKT-sikkerhet og investere tyngre fremover ved bestilling/kravsetting og utvikling av løsninger som tilfredsstiller kravene til innebygd personvern.

7.4.8 Tilsyn og kontroll med behandlingen av personopplysninger

Tilsyn og kontroll er nødvendige kontrollmekanismer for å sikre forsvarlig og lovlig behandling av personopplysninger.

Datatilsynet fører tilsyn med at politiets og påtalemyndighetens behandling av personopplysninger følger loven og forskrifter gitt i medhold av loven, og at feil eller mangler blir rettet.[121] PST er unntatt Datatilsynets tilsynskompetanse, idet tilsynskompetansen som tidligere nevnt ligger hos Stortingets eget kontrollutvalg for de hemmelige tjenestene (EOS-utvalget).[122] Datatilsynet kan iverksette tilsyn med behandling av personopplysninger etter politiregisterloven enten etter anmodning fra den registrerte (eller den som tror den er registrert), eller på eget initiativ.

Datatilsynets plikter å iverksette kontroll etter begjæring fra den registrerte, jf. politiregisterloven § 59. Bestemmelsen gir den registrerte en rett til å begjære en slik undersøkelse, noe som innebærer tilsvarende plikt for Datatilsynet til å undersøke om opplysningene om klageren er riktige, og om de er registrert og brukt i samsvar med loven. Tilsvarende rettighet tilkjennes den registrerte i medhold av SIS-loven § 21. Tilsynet *skal* iverksette undersøkelse av hvorvidt «opplysningene om vedkommende er behandlet i samsvar med loven og at reglene om innsyn er fulgt». Det stilles ikke krav om at klageordningen internt i politiet må være uttømt før man henvender seg til Datatilsynet, noe som betyr at den registrerte står fritt til å velge om vedkommende vil rapportere til tilsynet eller klage til overordnet organ i politiet.

Det finnes, så langt *Personvernkommisjonen* er kjent med, ikke offentlig tilgjengelig statistikk over antallet registrerte som benytter seg av denne retten til å klage. Datatilsynet opplyser i årsmeldingene for 2020 og 2019 at de har behandlet en rekke forespørsler om «innsyn i SIS», men uten at dette er tallfestet. Tilsvarende informasjon om bruk av tilsynsmyndighet på anmodning fra de registrerte etter politiregisterloven er ikke gitt.

Personvernkommisjonen mener Datatilsynet og politiet bør føre statistikk over antallet personer som årlig benytter seg av retten til å klage inn politiets behandling av personopplysninger. Offentliggjøring av slik statistikk kan bidra til å løfte bevisstheten om retten til å klage.

Datatilsynet kan videre igangsette tilsyn med behandling av personopplysninger etter politiregisterloven på eget initiativ. *Personvernkommisjonen* stiller spørsmål ved om Datatilsynet i tilstrekkelig grad benytter tilsynsmyndigheten de er gitt etter politiregisterloven. Ingen av de sentrale, bindende avgjørelsene som Datatilsynet trekker frem i sine årsrapporter i 2019 – 2021 gjelder justissektoren. Ingen av kontrollaktivitetene som er gjennomført de siste fem årene omhandler informasjonssikkerhet og internkontroll i forbindelse med behandling av personopplysninger etter politiregisterloven.

Personvernkommisjonen er imidlertid kjent med at Datatilsynet har gjennomført og planlegger tilsyn i justissektoren i 2022. I 2021 ble det gjennomført tilsyn med Kriminalomsorgsdirektoratet. *Personvernkommisjonen* anser det som viktig at Datatilsynet gjennomfører lovpålagt tilsynsarbeid på justisområdet.

Kommunikasjonskontrollutvalget

Kommunikasjonskontrollutvalget skal kontrollere at politiets bruk av kommunikasjonskontroll,

---

[120] Norges Domstoler. (u.å.). *Aktørportalen for advokater*.

[121] Politiregisterloven § 58, jf. Politiregisterforskriften § 42-1.

[122] Se omtale av EØS-utvalgets oppgaver og ressurser, samt effektiviteten av deres kontrollvirksomhet, i Datatilsynets høringsuttalelse til ny etterretningslov: Datatilsynet. (2019). *Høringsuttalelse fra Datatilsynet - Forslag til ny lov om etterretningstjenesten*.

romavlytting og dataavlesing skjer innenfor rammen av lov og instrukser, og at tvangsmiddelbruken begrenses mest mulig.[123] Utvalget behandler klager fra enkeltpersoner eller organisasjoner som mener seg urettmessig utsatt for kommunikasjonskontroll og kan også ta opp saker eller forhold i tilknytning til politiets og påtalemyndighetens bruk av kommunikasjonskontroll som det finner grunn til å behandle.

Personvernkommisjonen har ovenfor anbefalt at politiets metodebruk evalueres jevnlig, og *kommisjonen* anbefaler at det utvalget som får denne oppgaven også blir bedt om å vurdere om Kommunikasjonskontrollutvalget bør styrkes og mandatet utvides til å omfatte kontroll med andre av politiets metoder enn kommunikasjonskontroll, romavlytting og dataavlesning. En styrking av Kommunikasjonskontrollutvalget vil være et viktig supplement til andre rettssikkerhetsgarantier, som vurderinger av personvernkonsekvenser og domstolskontroll.

Personvernkommisjonen mener videre det er viktig at Kommunikasjonskontrollutvalgets sekretariat har kompetanse på personvern.

7.5 Personvernkommisjonens anbefalinger oppsummert

Behandlingsansvaret i kriminalomsorgen

- *Personvernkommisjonen* mener Justis- og beredskapsdepartementet, i arbeidet med ny lov om straffegjennomføring, bør tydeliggjøre behandlingsansvaret i kriminalomsorgen og legge ansvaret til den virksomhet som utfører den faktiske behandlingen av personopplysninger.

Internasjonalt samarbeid

- *Personvernkommisjonen* mener funnene EDPS har avdekket, om at EUROPOL mottar store mengder personopplysninger fra politiet i medlemsland, må følges opp av norske myndigheter for å sikre at personvernet til norske innbyggere blir ivaretatt når politiet overfører opplysninger til EUROPOL. *Kommisjonen* antar at tilsvarende problemstillinger kan foreligge i andre sammenhenger hvor informasjon utveksles mellom politimyndigheter, for eksempel mellom Norge og INTERPOL, og at dette også må følges opp.

Vurderinger av personvernkonsekvenser i lovarbeid

- *Personvernkommisjonen* mener departementene i større grad bør rådføre seg med Datatilsynet i forbindelse med lov- og forskriftsarbeid for å sørge for at personvernkonsekvenser drøftes i tilstrekkelig grad. En grundig vurdering av personvernkonsekvenser i lovarbeider er en forutsetning for demokratisk kontroll.
- *Personvernkommisjonen* mener regjeringen må bevilge midler til forskning på samfunnsmessige konsekvenser av overvåkningstiltak i justissektoren. Dette er viktig kunnskap for å være i stand til å gjøre helhetsvurderinger ved innføring av lovendringer.

Vurderinger av personvernkonsekvenser i myndighetsutøvelsen

- *Personvernkommisjonen* mener Justis- og beredskapsdepartementet må vurdere om alle bestemmelsene i politidirektivet skal implementeres i politiregisterloven. En harmonisering av loven med direktivet vil gi klarere retningslinjer for personvernvurderinger og gjøre det enklere for tjenestepersoner å anvende loven.
- *Personvernkommisjonen* mener bruk av åpne kilder på internett kan skape særskilte personvernutfordringer. *Kommisjonen* er blant annet bekymret for hvilke nedkjølingseffekter som kan oppstå som følge av justissektorens bruk av åpne kilder på nett, og dette perspektivet må vektlegges ved utarbeidelse av interne instrukser og lignende.
- *Personvernkommisjonen* mener at dersom det igangsettes tiltak som innebærer masseinnsamling av personopplysninger for nærmere angitte formål, er det viktig at metoder for dataseparasjon følges for å sikre at data kun benyttes til formål lovgiver har vurdert det nødvendig for.
- *Personvernkommisjonen* mener ledelsen i politiet må ha høy bevissthet om faren for formålsutglidning, og at risikoen for slik utglidning må reduseres gjennom etablering av organisatoriske og tekniske tiltak. Et viktig tiltak i denne sammenheng er å bygge en god personvernkultur. Dette er et lederansvar.

[123] Forskrift 9. september 2016 om kommunikasjonskontroll, romavlytting og dataavlesing (kommunikasjonskontrollforskriften) § 14.

Åpenhet

- *Personvernkommisjonen* anbefaler at det nedsettes et utvalg for å utrede metodebruken i justissektoren. Utvalget bør særlig vurdere personvernkonsekvenser av politiets metoder, særlig sett opp mot formålsprinsippet og proporsjonalitetsprinsippet. Dette arbeidet forutsetter at utvalget har tilgang på nødvendig informasjon om bruken av inngripende metoder og skjulte tvangsmidler. Dette er viktig både som et tillitsbevarende tiltak, og for å reise en åpen og demokratisk debatt om hvor grensen mellom personvern og kriminalitetsbekjempelse og forebygging bør gå.

Domstolskontroll

- *Personvernkommisjonen* mener det bør vurderes om dagens domstolskontroll av politiets tiltak bør utvides til å omfatte flere tiltak enn i dag. *Kommisjonen* understreker videre viktigheten av at bestemmelser som hjemler forskjellige tvangsmidler formuleres slik at effektiv og reell domstolskontroll blir mulig.
- *Personvernkommisjonen* mener det bør innføres et tillegg i straffeprosessloven § 170a som sikrer at det gjøres en vurdering av at den samlede bruken av ulike etterforskningsmetoder ikke blir et uforholdsmessig inngrep. I et slikt tillegg bør det understrekes at hensynet til personvern skal vektlegges ved denne vurderingen.

Særskilte problemstillinger knyttet til bruk av ny teknologi

- *Personvernkommisjonen* mener det er avgjørende med åpenhet og muligheter for kontroll ved anskaffelser i justissektoren. Ved anskaffelse av potensielt inngripende verktøy må personvernvurderinger være en sentral del av beslutningsgrunnlaget.
- *Personvernkommisjonen* mener det bør tas spesielt hensyn til etterprøvbarhet og ivaretakelse av den enkeltes rettigheter ved bruk av maskinlæringssystemer i justissektoren. For at slike metoder skal kunne tas i bruk i Norge, må de også være forklarbare for den som anvender teknologien, og risikovurderinger og pålagt teknisk dokumentasjon må foreligge i tråd med forslaget om forordning for kunstig intelligens.
- *Personvernkommisjonen* anbefaler et generelt forbud mot bruk av ansiktsgjenkjenning og annen biometrisk fjernidentifikasjon i offentlige rom. Et slikt forbud vil åpenbart begrense mulighetene for oppklaring av enkelte former for kriminalitet, men etter *kommisjonens* syn er teknologien såpass inngripende at det vanskelig kan forenes med grunnleggende rettigheter og samfunnsverdier.
- *Personvernkommisjonen* mener det er viktig at politiet settes i stand til å håndtere alvorlig kriminalitet, men dette bør skje med minst mulig inngrep i mulighetene for fri og sikker kommunikasjon. Mistankekrav og krav om klar og tydelig lovhjemmel og domstolskontroll ved inngrep må ligge fast.

Kompetanse

- *Personvernkommisjonen* kan ikke se at politiet i tilstrekkelig grad har vektlagt å øke medarbeidernes bevissthet rundt personvern. Personvernkompetanse og -kultur må forankres i ledelsen i politiet. Det må også vies ressurser til at personvernombud kan legge til rette for kompetanseheving i organisasjonen.
- *Personvernkommisjonen* mener tjenestepersoner i politiet bør ha grundigere opplæring i personvern enn det som i dag er tilfellet. Behovet er spesielt stort i forbindelse med bruk av IKT-systemer i det daglige politiarbeidet, ved personvern og menneskerettighetsvurderinger ved innhenting og utlevering av personopplysninger, og ved samarbeid med andre offentlige eller private virksomheter.
- *Personvernkommisjonen* mener personvernkompetansen i enhetene for digitalt politiarbeid (DPA) i politidistriktene bør styrkes, slik at alle operative beslutninger knyttet til elektronisk behandling av personopplysninger foregår innenfor eksisterende rettslige rammer for personvern, og etter robuste risikovurderinger. DPA-enhetenes samarbeid med personvernrådgivere og personvernombud i politiet må avklares og innarbeides mer enhetlig, gjerne gjennom nasjonale retningslinjer.
- *Personvernkommisjonen* mener undervisningen i personvern ved Politihøgskolen må styrkes. Politihøgskolen har en viktig oppgave i å bygge opp forståelse allerede i utdanningsløpet for viktigheten av personvern i politiets daglige arbeid.

Systemer og verktøy for å ivareta personvernet

- *Personvernkommisjonen* mener norske myndigheter bør innhente erfaringer fra andre land om ordninger for å filtrere bort overskuddsin-

formasjon ved beslag av digitale lagringsenheter og vurdere å etablere en lignende ordning. Personvernhensyn må alltid veies opp mot hensynet til oppklaring av kriminalitet der man i en dynamisk etterforskning ikke alltid i starten har full oversikt over hva slags informasjon som senere kan vise seg å få betydning som bevis.

- *Personvernkommisjonen* mener Justis- og beredskapsdepartementet bør etablere en samhandlingsplattform for dokumentutlevering i justissektoren. Plattformen bør utvikles med personvern og sikkerhet for øye, og bør blant annet ha funksjoner for å begrense muligheter for nedlasting og loggingsfunksjoner for å begrense urettmessig gjenbruk av dokumenter.
- *Personvernkommisjonen* mener Justis- og beredskapsdepartementet bør etablere en norm for IKT-sikkerhet og investere tyngre fremover ved bestilling/kravsetting og utvikling av løsninger som tilfredsstiller kravene til innebygd personvern.

Tilsyn og kontroll

- *Personvernkommisjonen* mener Datatilsynet og politiet bør føre statistikk over antallet personer som årlig benytter seg av retten til å klage inn politiets behandling av personopplysninger. Offentliggjøring av slik statistikk kan bidra til å løfte bevisstheten om retten til å klage.
- *Personvernkommisjonen* anbefaler at utvalget som er foreslått nedsatt for å vurdere personvernkonsekvenser av politiets metoder, også blir bedt om å vurdere om Kommunikasjonskontrollutvalgets mandatet bør utvides til å omfatte kontroll med andre av politiets metoder enn kommunikasjonskontroll, romavlytting og dataavlesning. En styrking av Kommunikasjonskontrollutvalget vil være et viktig supplement til andre rettssikkerhetsgarantier, som vurderinger av personvernkonsekvenser og domstolskontroll.

Kapittel 8
Personvern i skolen og barnehagen

8.1 Innledning

Personvernkommisjonen skal ifølge mandatet kartlegge «hvordan barn og unges personvern ivaretas i Norge.» Herunder skal *kommisjonen* kartlegge «ivaretakelse av barns personvern i barnehage- og skolesektorene og skolenes bruk av «gratis» applikasjoner der det betales med barnas personopplysninger.» *Kommisjonen* vurderer mandatets ordlyd som todelt, men overlappende.

Barn og unge i Norge tilbringer store deler av hverdagen i barnehage og skole. I løpet av barnehage- og grunnskoleløpet samles det inn og behandles store mengder informasjon om barna, inkludert mange personopplysninger. Som i andre samfunnssektorer har digitaliseringen av skole og barnehage gått fort, og den økende bruken av digitale hjelpemidler og verktøy har ført til at personopplysninger samles inn og behandles i stadig større grad. Barn har et særskilt krav på beskyttelse, og har i hovedsak ikke muligheten til å velge bort de digitale løsningene. Dette betyr at det er særdeles viktig at personvernet er på plass før verktøy tas i bruk.

Skole- og barnehagesektorenes behandling av personopplysninger er nødvendig for å sikre et godt utdanningsløp, men forutsetter gode systemer og rutiner for å sikre ansvarlig behandling av opplysningene. I norske skoler tas det i bruk digitale verktøy i utstrakt grad. Disse verktøyene er ofte levert av private aktører. I mange tilfeller er disse aktørene store internasjonale teknologiselskaper, hvor skoleadministrasjonen og kommunene har få eller ingen muligheter til å påvirke selskapenes behandling av personopplysninger. Utdanningssektoren er et attraktivt marked for disse selskapene, blant annet fordi det gjør det mulig å skape tidlige forbrukerrelasjoner med elevene. Utviklingen medfører at både administrasjon, lærere og barn kan få tilgang til nyttige tjenester, men den kan også ha negative konsekvenser for personvern og IKT-sikkerhet.

Personvernkommisjonen erfarer at det er betydelige forskjeller mellom kommunene og den enkelte skole og barnehage når det gjelder både bruk av digitale verktøy og ivaretagelse av personvern. Det eksisterer få nasjonale retningslinjer for hvordan digitaliseringen i sektoren skal gjennomføres på en personvernvennlig måte, og mange skoler og kommuner har begrensede midler og kompetanse til å ivareta sitt ansvar på feltet. I verste fall kan dette føre til at skoler og barnehager tar i bruk verktøy uten at det gjennomføres kvalitetskontroll av nytteverdien eller foretas vurderinger av konsekvenser for personvernet. Det kan medføre at barns personopplysninger kommer på avveie eller blir en handelsvare for internasjonale teknologiselskaper. *Personvernkommisjonen* mener at kommersiell utnyttelse av elevers personopplysninger er uakseptabelt.

For barn og unge i skolen, handler personvern om at foreldre og barn skal vite om og ha kontroll over hvordan opplysningene om barna blir brukt. Barnehagene og særlig skolene har også ansvar for opplæring som sørger for at barn settes i stand til å forstå og håndtere praktiske utfordringer og viktige samfunnsaspekter. Det bør etter *kommisjonens* syn også innebære grunnleggende opplæring i personvern i både praktisk og samfunnsfaglig forstand. En grunnleggende forståelse av personvern vil være en forutsetning for å ha en helhetlig forståelse av digitaliseringen nå og i tiden fremover.

I dette kapitlet vil *Personvernkommisjonen* beskrive hvordan barns personvern ivaretas i skole og barnehage i dag, og peke på hvilke utfordringer som oppstår ved behandling av barns personopplysninger. *Kommisjonen* vil si noe om hvilke faktorer som bidrar til at personvernet til elever og barnehagebarn er under press, herunder den hurtige digitaliseringen, mangel på kompetanse, etterlevelse av ansvaret for personvern, økt innsamling av personopplysninger og påvirkning fra de store globale aktørene.

8.1.1 Avgrensninger, begreper og definisjoner

Personvernkommisjonen har hovedfokus på problemstillinger knyttet til ivaretakelsen av barns personvern i grunnskolen. Mange av utfordringene i grunnskolen gjør seg imidlertid også gjeldende både i barnehagen og i videregående opplæring. Flere av vurderingene og tiltakene som gjelder grunnskolen vil derfor også ha relevans for behandlingen av personopplysninger i barnehagen og i videregående opplæring.

Personvernkommisjonen skal ifølge mandatet se på skolens bruk av «gratis» applikasjoner der det betales med barns personopplysninger. *Applikasjoner* forstår *kommisjonen* som teknologi som brukes i skolen, mer presist som digitale læringsressurser og læringsplattformer. *Digitale læringsressurser* omfatter verktøy for elevproduksjon, innholdsressurser og digitale læremidler.[1] En *digital læringsplattform* er en arena for å opprette, dele, kommunisere, analysere og administrere innhold for bruk i opplæringen, som eksempel plattformen itsLearning.[2]

Både digitale læringsressurser og læringsplattformer omtales nedenfor samlet som digitale *læringsverktøy*. Digitale læringsverktøy omfatter med andre ord alle digitale verktøy som brukes av lærerne og elevene som en del av skolehverdagen. Digitale læringsverktøy kan leveres av både offentlige og private aktører, og det vil variere i hvilken grad verktøyene krever behandling av personopplysninger. Enkelte verktøy vil nødvendigvis behandle store mengder personopplysninger for å kunne levere sin funksjonalitet, mens andre verktøy trenger å behandle få eller ingen personopplysninger for å fungere. I tillegg behandler noen digitale læringsverktøy personopplysninger for andre formål eller utover det som er nødvendig for å levere tjenesten. Dette er særlig problematisk fra et personvernperspektiv. Innenfor kommersiell sektor kalles digitale læringsmidler gjerne «edtech».

Det følger videre av mandatet at *Personvernkommisjonen* ikke skal «foreslå tiltak som innebærer endringer i læreplanverket Kunnskapsløftet 2020.» *Kommisjonen* vil av denne grunn ikke gå nærmere inn på spørsmål om endringer i læreplanen.

I 2021 opprettet Kunnskapsdepartementet en ekspertgruppe for digital læringsanalyse. Gruppen består av eksperter innen skole og utdanning, samt fagområder som etikk, teknologi og jus. Ekspertgruppen er nedsatt for å gi Kunnskapsdepartementet bedre grunnlag for beslutninger om digital læringsanalyse og adaptive læremidler, prøver og tester i grunnopplæringen, høyere utdanning og høyere yrkesfaglig utdanning. Ifølge mandatet skal ekspertgruppen, i tillegg til å vurdere pedagogiske spørsmål ved bruk av digital læringsanalyse, også vurdere etiske og juridiske spørsmål og problemstillinger knyttet til personvern.[3]

Læringsanalyse kan gi den enkelte bedre og mer tilrettelagt undervisning, men storstilt innsamling, lagring og analyse av elevopplysninger kan også medføre personvernutfordringer. Det er blant annet personvernutfordringer knyttet til formålsutglidning, manglende transparens, risiko for ukorrekte personopplysninger i systemet og at elevene endrer atferd (nedkjølingseffekt).

Ekspertgruppen skal ifølge mandatet ha kontakt med *Personvernkommisjonen*. *Kommisjonen* har hatt møter med ekspertgruppen for å gjøre avgrensninger der det er sammenfall i mandatene. Ettersom ekspertgruppen skal se nærmere på ivaretakelse av personvernet i systemer for digital læringsanalyse, har *Personvernkommisjonen* avgrenset sitt mandat fra å gå dypt inn i denne problematikken. *Personvernkommisjonen* vil likevel kommentere utfordringer ved denne teknologien der det er relevant utover i kapitlet.

8.1.2 Politiske føringer for personvern i skolen og barnehagen

Staten har det overordnede ansvaret for utviklingen av skole- og barnehagesektoren og for å sikre ivaretakelse av elevenes og barnehagebarnas grunnleggende rettigheter. Staten har også det overordnede ansvaret for digitalisering av det offentlige, herunder skolesektoren. Nasjonale myndigheter har imidlertid ikke det juridiske ansvaret for å ivareta personvernet til barn i skole og barnehage. Behandlingsansvaret for elevenes personopplysninger ligger til kommunene.

Statlige myndigheter har likevel mulighet til å påvirke ivaretakelsen av barns personvern i skolen og barnehagen på flere ulike måter. Kunnskapsdepartementet har ansvar for å styre grunn-

[1] Definisjon er hentet fra Handlingsplan for digitalisering i grunnopplæringen. Kunnskapsdepartementet. (2020–2021). *Handlingsplan for digitalisering i grunnopplæringen.*

[2] Utdanningsdirektoratet. (2021, 12. mars). *Læringsmidler og læringsteknologi i skole og opplæring.*

[3] Kunnskapsdepartementet. (2021). *Mandat for ekspertgruppe som skal vurdere bruk av læringsanalyse i grunnopplæringen, høyere yrkesfaglig utdanning og høyere utdanning.*

opplæringen. Utdanningsdirektoratet har ansvar for å utvikle læreplaner for skolen og rammeplan for barnehagen. Læreplanene påvirker først og fremst selve innholdet i undervisningen, men også til en viss grad utvelgelse av hvilke digitale verktøy som er egnet til bruk i undervisningen. Utforming av læreplanene påvirker elevenes personvern, da de kan legge føringer for hva barna lærer om personvern i skolen, og hvilke verktøy som brukes i undervisningen og som kan samle inn personopplysninger om barna. Staten har også mulighet til å påvirke ivaretakelsen av elevenes personvern gjennom å sette vilkår rettet mot ivaretakelse av personvern i ulike statlige tilskuddsordninger for utvikling og innkjøp av digitale læringsverktøy.

I 2017 lanserte Kunnskapsdepartementet «Digitaliseringstrategi for grunnopplæringen 2017–2021».[4] Strategien har to hovedmål: Elevene skal ha digitale ferdigheter som gjør dem i stand til å oppleve livsmestring og lykkes i videre utdanning, arbeid og samfunnsdeltakelse og IKT skal utnyttes godt i organiseringen og gjennomføringen av opplæringen for å øke elevenes læringsutbytte.

Personvern og informasjonssikkerhet inngår som en av fem hovedprioriteringer i strategien. Skolesektorens arbeid med personvern og informasjonssikkerhet skal være et mål i seg selv, som viktig kunnskap elevene må ha for å kunne være bevisste og kritiske digitale borgere. Personvern og informasjonssikkerhet er også løftet frem som viktige hensyn skolen må ivareta i digitaliseringsarbeidet: «Godt personvern og god informasjonssikkerhet har konsekvenser for både innholdet i læreplanene og for forvaltningen av elevenes og lærernes personopplysninger». Strategien peker på at kompetanse om personvern og informasjonssikkerhet vil bli stadig viktigere når både læremidler og administrative systemer blir mer komplekse.

Digitaliseringsstrategien følges opp og utdypes i *Nasjonal handlingsplan for digitalisering i grunnopplæringen 2020 – 2021.*[5] Handlingsplanen er utarbeidet av Kunnskapsdepartementet med innspill fra blant andre Kommunesektorens organisasjon (KS) og representanter fra kommunesektoren, lærerorganisasjonene, Elevorganisasjonen, IKT-Norge, Forleggerforeningen, Foreldreutvalget for grunnopplæringen (FUG), Sametinget og Nasjonal digital læringsarena (NDLA).

Handlingsplanen for digitalisering i grunnopplæringen trekker frem nødvendige tiltak som bør gjennomføres i skolesektoren i perioden 2020–2021. Tiltakene omfatter å sikre tilgang til digitale ressurser og kompetanse hos lærere og kommuner i bruk av teknologi i skolen. I tillegg er det identifisert en rekke tiltak for å sikre at elevenes personvern er godt ivaretatt når deres personopplysninger behandles i administrative og pedagogiske verktøy. Disse tiltakene går ut på å øke veiledningen om personvern ut mot skolesektoren, samt nedsette en ekstern ekspertgruppe for å utrede pedagogiske, juridiske, teknologiske og etiske problemstillinger knyttet til læringsanalyse og eierskap til elevdata i skolen. Ekspertgrupppen er omtalt i avsnitt 8.1.1.

Det fremgår av tildelingsbrevet til Utdanningsdirektoratet for 2021 at det skal iverksettes følgende tiltak i handlingsplanen, med relevans for personvernet:

- Utrede og utvikle en pilot for en nasjonal tjenestekatalog for digitale læremidler.
- Øke den generelle veiledningen på personvern ut mot sektoren, for eksempel ved å publisere maler og eksempler på utfylling av disse (beste praksis).
- Lage generell veiledning om hvilke krav som bør stilles til leverandører når det gjelder personvern og informasjonssikkerhet.
- Øke veiledningen om personvern på spesifikke områder innen skolesektoren, for eksempel skolemiljø, spesialundervisning og andre områder hvor skolen håndterer sensitive personopplysninger i forbindelse med elevers individuelle rettigheter.

Personvernkommisjonen forstår disse tiltakene slik at departementet ønsker å gi Utdanningsdirektoratet en tydeligere veilederrolle for kommunene på personvernområdet. I tildelingsbrevet til Utdanningsdirektoratet for 2022 skriver Kunnskapsdepartementet at en av de overordnede prioriteringene for 2022 er digital kompetanse og digitalisering, herunder å sørge for bruk av digitale løsninger med godt personvern.[6] Tiltakene er videre ment å sette i gang viktige prosesser inn mot ny «Digitaliseringsstrategi for grunnopplæringen» som vil gjelde fra 2022.

Personvernkommisjonen vil særlig trekke frem forslaget om å opprette en nasjonal tjenestekata-

[4] Kunnskapsdepartementet. (2017). *Framtid, fornyelse og digitalisering. Digitaliseringsstrategi for grunnopplæringen 2017–2021.*

[5] Kunnskapsdepartementet. (2020). *Handlingsplan for digitalisering i grunnopplæringen 2020–2021).*

[6] Kunnskapsdepartementet. (2021). *Arbeidsdokument tildelingsbrev til Udir for 2021.*

log som et viktig initiativ som kan styrke personvernet til elevene i skolen dersom krav til personvern og IKT-sikkerhet legges til grunn som et kriterium for vurdering av tjenesten som skal inn i tjenestekatalogen. Forslaget om en nasjonal tjenestekatalog vil bli nærmere diskutert i avsnitt 8.4.1.

8.1.3 Tillit til skolens behandling av personopplysninger

Datatilsynets personvernundersøkelse fra 2019/2020 viser at tilliten til hvordan skoler og barnehager ivaretar barnas personvern er relativt lav, vesentlig lavere enn til andre offentlige etater. Bare 56 % svarer at de har tillit til hvordan skoler og barnehager oppbevarer og bruker personopplysninger.[7] Med tanke på hvor sensitive opplysninger skolen har ansvar for, er det god grunn til å rette særlig oppmerksomhet mot hvordan personvernet til barn i skolen og barnehagen ivaretas.

I løpet av de siste årene har en rekke skoleeiere mottatt gebyrer fra Datatilsynet for brudd på personopplysningsloven. Siden 2019 har norske skoleeiere fått gebyrer i millionklassen for brudd på personopplysningssikkerhet i mobilapplikasjonen Skolemelding,[8] i administrative systemer[9] og systemer for kommunikasjon mellom skole og hjem.[10] Mindre gebyrer har blitt utstedt for å behandle helseopplysninger om barn i læringsplattformen Showbie,[11] og i 2021 ble det ilagt et gebyr på 50 000 kr for bruk av treningsapplikasjonen Strava i undervisningen uten at det var gjennomført en personvernkonsekvensvurdering.[12] I 2020 fikk tre kommuner varsel om irettesettelse fra Datatilsynet for deres bruk av Googles løsninger i skolen.[13]

Det har vært mye medieoppmerksomhet rundt disse sakene, som antageligvis har bidratt til å øke oppmerksomheten på personvern i sko-

7 Datatilsynet. (2019). *Personvernundersøkelsen 2019/2020.*

8 Datatilsynet. (2019). *Gebyr til Oslo kommune Utdanningsetaten.*

9 Datatilsynet. (2019). *Endelig vedtak om gebyr til Bergen kommune.*

10 Datatilsynet. (2020, 9. september). *Endelig vedtak* om gebyr til Bergen kommune.

11 Datatilsynet. (2020, 10. juli). *Endelig vedtak* om gebyr til Rælingen kommune.

12 Datatilsynet. (2021). *Gebyr til Ålesund kommune for bruk av Strava.*

13 Datatilsynet. (2020). *Varsel om irettesettelse for feil bruk av Googles løsninger i skolen.*

Boks 8.1 Mangel på retningslinjer og rutiner

Vigilo-saken

I september 2020 ble det i Bergen kommune avdekket alvorlig sikkerhetssvikt i skoleappen Vigilo. Appen brukes til kommunikasjon mellom foreldre og ansatte i skoler og barnehager og skulle effektivisere blant annet barnehageopptak, føring av fravær og kommunikasjon med foreldre. Problemene bestod blant annet i at foreldre med besøksforbud hadde fått tilgang til opplysninger om sine barn i appen. I tillegg ble foreldre uten foreldreansvar automatisk lagt til i appen. Datatilsynet understreket at kommunen ikke hadde etablert og kommunisert nødvendige retningslinjer for opplysninger om barn ved etablering av Vigilo. Datatilsynet ga et overtredelsesgebyr til Bergen kommune på 3 millioner kroner som kommunen aksepterte.[1]

Showbie-saken

Rælingen kommune ble ilagt et overtredelsesgebyr på 500 000 kroner for ikke å ha foretatt risikovurderinger, vurderinger av personvernkonsekvenser og testing før applikasjonen Showbie ble tatt i bruk. Showbie ble brukt til å kommunisere helserelaterte personopplysninger mellom skole og hjem. Overtredelsen omfattet elever ved en tilrettelagt avdeling ved en skole. Mangelfull sikkerhet ved innlogging i applikasjonen gjorde det mulig å få tilgang til andre elever i gruppen. Kommunen påpekte at det ikke var noe i saken som tydet på at noen av barna/elevene rent faktisk hadde vært utsatt for materiell eller ikke-materiell skade. Datatilsynet understreket i vedtaket at «selve sikkerhetsbruddet utgjorde en risiko, uavhengig av om risikoen manifesterer seg i en mer konkret form for skade for de berørte eller ikke».[2]

1 Datatilsynet. (2020, 9. september). *Endelig vedtak om gebyr til Bergen kommune.*

2 Datatilsynet. (2020, 10. juli). *Endelig vedtak om gebyr til Rælingen kommune.*

len og i kommunene rundt om i landet. Oppmerksomheten kan også ha vært utslagsgivende for at tilliten til skolers behandling av personopplysninger er relativt lav.

Datatilsynet har i Personvernundersøkelsen 2019/2020 pekt på at norske kommuner «har en jobb å gjøre når det gjelder å sikre at barns personvern blir ivaretatt i skolen». Skolesektoren har de siste årene rapportert et økende antall brudd på personopplysningssikkerheten til Datatilsynet.[14] En fellesnevner for disse sakene er at det er gjort mangelfulle risikovurderinger og at løsningene ikke er blitt tilstrekkelig testet, før de implementeres og tas i bruk. I etterkant av en rundebordskonferanse i februar 2021 uttrykte likevel Datatilsynet at det er tatt mange gode initiativer, og at personvern i skolen tas på mye større alvor nå enn for bare noen år siden.[15]

Kommunesektorens organisasjon (KS) har gitt innspill til *Personvernkommisjonen* om at de er svært bekymret for situasjonen for personvernet i norsk skole. *Personvernkommisjonen* deler denne bekymringen og stiller spørsmål om hvilken pris det har hatt for elevenes personvern at den digitale utviklingen i skolen har gått så raskt, uten at det har vært gjort tilstrekkelige vurderinger eller tiltak for å sikre personvernet.

8.2 Digitale løsninger i skolen

Det kommunale selvstyret står sterkt i Norge. I skolesektoren innebærer det at avtaler om hvilke digitale løsninger som tas i bruk for læring, kommunikasjon og elevvurdering, i stor grad forhandles frem i hver enkelt kommune.

Skole- og barnehageledelsen har ansvaret for oppfølging av lære- og rammeplan, og spesifiserer dermed hvilke behov for digitale læringsverktøy de har i oppgaveløsningen. Det er skole- og barnehageeier (kommunen) som gjør innkjøp av digitale læringsverktøy og som har behandlingsansvaret. Det er også kommunen som vurderer hvilke opplysninger som skal behandles og hvordan opplysninger skal lagres. Det er store forskjeller mellom skolene og barnehagene, både når det gjelder hvilke løsninger som velges og hvordan disse tas i bruk.

8.2.1 Hvilke applikasjoner blir elevene registrert i?

Kommunesektorens organisasjon (KS) har, på oppdrag fra *Personvernkommisjonen*, laget en rapport med oversikt over hvilke systemer og løsninger som lagrer personopplysninger om elevene.[16]

Disse systemene og løsningene kan deles inn i følgende hovedkategorier: *administrative verktøy*, *applikasjoner* og *programvare* og *plattformer*, som illustrert nedenfor.

8.2.1.1 Administrative verktøy

Administrative verktøy omfatter skoleadministrative systemer, kommunikasjonsløsninger for eksterne, evalueringssystemer og tekniske støtteverktøy.

Skoleadministrative systemer er tekniske løsninger for å ivareta forskjellige administrative prosesser knyttet til både lærere, elever og foresatte. De største leverandørene av skoleadministrative systemer i Norge er Visma, Vigilo, TietoEvry Education og IST. Slike systemer samler inn et bredt spekter av personopplysninger knyttet til elevens skolegang, inkludert sensitive personopplysninger. Opplysninger kan samles inn av leverandørene, tredjeparter (for eksempel skylagringsleverandører) og kommuneadministrasjonen. Opplysningene samles blant annet inn fra folkeregisteret, sak- og arkivløsninger i kommunene, fra elevene og deres foresatte, samt fra lærerne.

Kommunikasjonsløsninger for eksterne er i hovedsak digitale verktøy for kommunikasjon mellom skole og foresatte. Typiske eksempler på slike kommunikasjonsløsninger er Visma, Vigilo, IST, TietoEvry Education, Zoom, Microsoft Teams, Google Workspace, itsLearning, Canvas, Fronter og Showbie. Ifølge KS anvendes sosiale medier som Facebook også i kommunikasjon mellom skole og foresatte, men dette er som regel ikke autorisert eller initiert av skoleeier.

Formalisert kommunikasjon mellom skole og foresatte foregår som regel gjennom skolens skoleadministrative system, og informasjonen som formidles der avhenger typisk av elevens alder. Informasjonen som formidles til foresatte gjennom slike systemer kan inkludere fravær, orden og oppførsel, samt karakterer og undervisningsvurderinger. Slik informasjon kan også kommuniseres gjennom skolens LMS (Learning Manage-

[14] Datatilsynet. (2019). *Personvernundersøkelsen 2019/2020.*

[15] Datatilsynet. (2021, 11. februar). *På rett veg i skolesektoren.*

[16] KS. (2022). *Personopplysninger i skolen.* Utredning på oppdrag fra Personvernkommisjonen.

Figuren bygger på en illustrasjon i rapporten Personopplysninger i skolen. Innspill til Personvernkommisjonen, Kommunesektorens organisasjon (februar 2022).

Figur 8.1

ment System) som for eksempel itsLearning, Canvas og Fronter. I slike kommunikasjonsløsninger samles det som regel inn opplysninger om elevens oppførsel og fravær, samt karakterer og vurderinger av elevens prestasjoner. Opplysningene samles inn av leverandørene av kommunikasjonsløsningen, og innhentes fra elever og deres foresatte, lærerne og skoleadministrasjonen.

Under pandemien har andre kommunikasjonsverktøy og produksjonsverktøy som Zoom, Microsoft Teams og Google Workspace blitt tatt i bruk for kommunikasjon mellom skole og foresatte, for eksempel i foreldremøter og utviklingssamtaler. KS erfarer også at det er en utstrakt bruk av sosiale medier for kommunikasjon mellom foresatte og skoleansatte. Slik bruk er som regel ikke forvaltet og organisert av skoleeier eller skoleleder. Det vil variere i stor grad hvilke personopplysninger som samles inn av slike plattformer, men det kan inkludere elevopplysninger, samt et vidt spekter andre opplysninger ved bruk av plattformer som Facebook og Google.

Evalueringssystemer er digitale løsninger som brukes for å evaluere elever, for eksempel for karaktersetting, tilpasset læring og elevundersøkelser. Slike systemer inkluderer for eksempel itsLearning, Canvas og Showbie, men løsninger som Microsoft 365 og Google Workspace anvendes også. Evalueringssystemer samler inn opplysninger om blant annet elevenes fravær, orden og oppførsel. Personopplysningene samles inn av løsningsleverandørene, skoleadministrasjonen og kommuneadministrasjonen, og hentes fra elevene og lærerne.

Under evalueringssystemer inngår også systemer for tilpasset læring, såkalte *adaptive læringsmidler*. Adaptive læringsmidler er en betegnelse på systemer for læringsanalyse, som samler inn og analyserer elevenes arbeid, resultater og behov. Formålet er å kartlegge og tilpasse læringsoppgaver og undervisning til elevenes kunnskapsnivå og prestasjoner, samt å identifisere elever som står i fare for å havne på etterskudd eller utenfor, slik at forebyggende tiltak kan iverksettes på et tidlig tidspunkt. Det kan innebære tilpasning på individnivå for den enkelte elev, eller på klasse-, skole-, eller skoleområdenivå.

Som med andre digitale analysesystemer, forutsetter bruken av adaptive læringsmidler som regel behandling av store mengder personopplysninger knyttet til enkeltelevers prestasjoner. Personvernkonsekvensene ved bruk av slike verktøy behandles av ekspertgruppen for digital læringsanalyse, og *Personvernkommisjonen* vil følgelig ikke gjøre en dybdevurdering av dette.[17]

8.2.1.2 Applikasjoner og programvare

Applikasjoner og programvare er tredjeparts læringsprogrammer som lastes ned på elevenes nettbrett eller PC for bruk i undervisningen. Slike programmer kan inkludere applikasjoner til bruk i matematikk, skrive- og leseundervisning, og kreative applikasjoner som brukes til innholdsproduksjon. Eksempler på slike programmer er Book Creator, Explain Everything, iMovie, Garageband, Dragonbox, Kahoot og Kidspiration. Andre tredjeparts programmer som anvendes i skolen inkluderer blant annet Microsoft 365, Google og Showbie.

Det vil i stor grad variere hvilke personopplysninger slike løsninger samler inn og hvordan personopplysningene viderebehandles, både utfra funksjonalitet og hensikten til applikasjonene, og forretningsmodellen til leverandøren. Dersom leverandøren har en forretningsmodell basert på innsamling og salg av personopplysninger, kan det være snakk om behandling av store mengder personopplysninger utover det som er nødvendig for å levere tjenesten og som kan deles med mange tredjeparter. Som beskrevet i kapittel 9 om forbrukernes personvern, kan slike applikasjoner inneholde sporingsteknologi som samler inn alt fra lokasjon og identifikatorer til interesser og historikk.

8.2.1.3 Plattformer

I sin rapport beskriver KS plattformer som både *systemløsninger* som for eksempel Google og Microsofts læringsløsninger, og *hardware* som Apple iPad eller Google Chromebook. Systemløsningene inkluderer operativsystemer og lagringsløsninger, samt verktøy for innholdsproduksjon og kommunikasjon. Eksempler på systemløsninger er kommunikasjonsplattformer som Gmail og Microsoft Teams, innholdsproduksjonsplattformer som Microsoft Word/PowerPoint og Google Docs, og nettnavigasjonsverktøy som Google Chrome, Safari og YouTube. I tillegg brukes Apples programvarepakker som leveres med iOS-operativsystemet, som blant annet inkluderer iMovie, Garageband, Keynote, Pages og Numbers.

Det er per i dag ikke noen tilgjengelige tall på den konkrete utbredelsen av forskjellige hardwa-

[17] Kunnskapsdepartementet. (2021). *Mandat for ekspertgruppe som skal vurdere bruk av læringsanalyse i grunnopplæringen, høyere yrkesfaglig utdanning og høyere utdanning.*

reløsninger i norske skoler, men KS anslår at de største leverandørene er Apple (iPad), Google (Chromebook), samt Microsoft (Windows PC). Noen kommuner har valgt å anskaffe kun én type plattformløsning til elevene, mens andre tar i bruk flere forskjellige. Ifølge tall fra Grunnskolens informasjonssystem (GSI)[18] for skoleåret 2020/2021, har blant landets 634 674 elever i grunnskolen 27 % egen bærbar PC eller Mac, 21 % har egen Chromebook, 40 % har nettbrett (iPad eller annet), mens 11 % har ikke tilgang til egen digital enhet.[19]

Plattformer kan samle inn store mengder personopplysninger, både gjennom selve maskinene (hardware) og ved forhåndsinstallerte programvareløsninger. I tillegg kan operativsystemene samle inn personopplysninger og annen brukerinformasjon på tvers av tjenester på enhetene. Opplysningene samles typisk inn av leverandørene, som Google, Microsoft og Apple.

8.2.2 Prosess for anskaffelse av digitale løsninger i skolen

KS beskriver i rapporten utarbeidet for *Personvernkommisjonen* følgende prosess for hvordan digitale verktøy og løsninger anskaffes i skolen[20]: Systemer og applikasjoner som brukes av alle skoler i en kommune, for eksempel et fagsystem, anskaffes gjerne med en «kommune-lisens». Dette innebærer ofte lengre anskaffelsesprosesser, og systemene vurderes ut fra kravspesifikasjoner. Enkelte kommuner anskaffer slike systemer gjennom regionale samarbeid og IKT-samarbeid.

Ved anskaffelse av enklere digitale læremidler og applikasjoner til bruk ved den enkelte skole, foregår anskaffelsen som regel gjennom drøftinger og vurderinger på trinnledermøter internt ved skolen, eller på ledermøter hvor alle skolene i kommunen er representert. I enkelte kommuner involverer dette innspillsrunder via faggrupper, mens endelig godkjenning og prioriteringer skjer på enhetsledernivå (for eksempel rektor) med delegert myndighet fra kommunedirektøren.

I rapporten beskriver KS bestillingsrutinene i kommunene som relativt like på flere punkter: I forbindelse med en anskaffelse gjøres det en pedagogisk vurdering av hvordan læremidlet kan hjelpe skolen/klassen/eleven i læringsarbeidet. Etter å ha gjennomført innspillsrunder med skolene og/eller lærerne, beslutter skoleeier anskaffelse av applikasjonen eller læremidlet på skoleeiernivå.

Som en del av bestillingsrutinen gjøres det en vurdering av hvordan personvernet ivaretas i applikasjonen, og flere kommuner stiller krav om at risiko- og sårbarhetsvurdering (ROS) og eventuelt en vurdering av personvernkonsekvenser (DPIA), gjennomføres før anskaffelsen. Likevel melder KS om at flere kommuner påpeker at manglende ressurser og kapasitet gjør at slike vurderinger trekker ut i tid, til etter at anskaffelsen er gjennomført.

Ved anskaffelser av applikasjoner vektlegger kommunene som regel krav om å oppfylle lovpålagte forpliktelser, for eksempel tilknyttet krav i opplæringslov og læreplaner, eller elevadministrative oppgaver. For skolene er det som oftest pedagogiske og didaktiske begrunnelser som vektes tyngst. Viktige faktorer for skolene inkluderer faglig nytteverdi, kvalitet, brukervennlighet, sikkerhet, pris, og erfaringer fra andre som har brukt applikasjonen. Kravene som stilles i personvernregelverket blir sjeldent sett på av skolen eller lærerne, og personvernvurderinger blir således en del av «siste skanse» før endelig anskaffelsesbeslutning tas.

8.3 Rettslige rammer for behandling av opplysninger i skole og barnehage

Skolens og barnehagens oppgaver følger av barnehageloven, opplæringsloven og privatskoleloven (tidligere friskolelova), som setter rammer for hvilke og hvordan personopplysninger kan behandles. I tillegg regulerer personvernforordningen behandling av barns personopplysninger, også i skole og barnehage. Barnehage- og opplæringsloven supplerer forordningen på de områdene der det etter forordningen er gitt adgang til nasjonal regulering, se nærmere kapittel 10 om nasjonalt handlingsrom.

Det rettslige grunnlaget for behandling av barns og unges personopplysninger i skole og barnehage er i hovedsak at behandlingen er nødvendig for å oppfylle en rettslig forpliktelse,[21] eller at behandlingen er nødvendig for å utføre en opp-

---

[18] Grunnskolens informasjonssystem (GSI) er Norges offisielle oversikt over grunnskoleundervisningen i landet, og er den viktigste kilden til grunnskoledata i Norge. GSI samler inn en omfattende mengde data om grunnskolen i Norge, inkludert digitale enheter i skolen. Utdanningsdirektoratet. (2021, 16. desember).

[19] KS. (2022). *Personopplysninger i skolen.* Utredning på oppdrag fra Personvernkommisjonen.

[20] KS. (2022). *Personopplysninger i skolen*. Utredning på oppdrag fra Personvernkommisjonen.

gave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt.[22] Behandling av «særlige kategorier av personopplysninger» skjer som oftest i henhold til forordningens artikkel 9 nr. 2 bokstav g. Opplæringslova, privatskoleloven og barnehageloven gir supplerende regler.

Den første august 2021 ble barnehageloven,[23] opplæringslova[24] og daværende friskolelova[25] endret, for å gi hjemmel til behandling av personopplysninger og gjennomføring av opplæring gjennom fjernundervisning.[26] Disse lovene er *teknologinøytrale*, det vil si at de ikke gir føringer på hvilken teknologi barnehage og skole skal bruke for å løse de angitte oppgavene. Lovene angir hvilke plikter kommune og den enkelte skole og barnehage har, og presiserer barnehagebarnas, elevenes og foreldrenes rettigheter.

Lovendringene innfører generelle bestemmelser om behandling av personopplysninger. Utformingen er tilnærmet lik i alle de tre ovennevnte lovene. Etter de respektive lovene kan det behandles personopplysninger, inkludert særlige kategorier av personopplysninger og opplysninger om straffedommer og lovovertredelser, «når det er nødvendig for å utføre oppgaver etter loven». Med «oppgaver» menes både plikter og oppgaver som kommunene er pålagt i og med hjemmel i lov, som er særlig regulert i de ovennevnte lovene.[27] For en nærmere gjennomgang viser *Personvernkommisjonen* til Prop. 145 L (2020–2021) *Endringar i opplæringslova, friskulelova og barnehagelova (behandling av personopplysningar, fjernundervisning o.a.)*.[28]

I personvernregelverket vurderes barn som en spesielt sårbar gruppe. Dette innebærer at barns personopplysninger er opplysninger om sårbare personer. I tillegg har ikke barn mulighet til å velge om de skal gå i barnehage eller på skole. Barna og deres foreldre er avhengige av at de ansvarlige både behandler data og ivaretar deres personvern ved gjennomføring av lovpålagte oppgaver. Siden barn i liten grad kan sette premissene for hvordan deres personopplysninger behandles, er de gitt særskilt beskyttelse i personvernregelverket. Dette betyr at behandlingsansvarlige også må gjøre særskilte vurderinger når de behandler opplysninger om barn. Disse vurderingene bør også dokumenteres.

8.3.1 Ansvarsplassering

Kommunen er *skole-* og *barnehageeier*, med unntak av privateide skoler og barnehager. Kommunen har ansvar for grunnskoleopplæring for alle som er bosatt i kommunen.[29] I tillegg har kommunen ansvaret for organisering og drift av skolen, herunder økonomisk ansvar, innenfor nasjonale føringer som blant annet lov, forskrift og læreplanverk.[30]

Kommunen anses som *behandlingsansvarlig* etter personvernforordningen og e-forvaltningsforskriften,[31] og har ansvaret for at personopplysningene til elever og barnehagebarn blir behandlet i tråd med forordningen.

Flere barnehager og skoler er privateide. Når det gjelder disse barnehagene og skolene, vil skolen eller barnehagen (den juridiske personen)være behandlingsansvarlig etter personvernforordningen for den behandling av personopplysninger som skjer i driften av virksomheten. Behandlingsansvaret i forbindelse med opptak og tildeling av skole- eller barnehageplass ligger hos kommunen.

Det er kommunen som har ansvaret for elevenes læremidler, blant annet å anskaffe digitalt utstyr.

Som behandlingsansvarlig er det kommunens ansvar at verktøy som anskaffes og benyttes i skole og barnehage, oppfyller personvernforordningens regler om personvern og informasjonssikkerhet. Herunder ligger en forpliktelse til å gjøre risikoanalyser og vurdere personvernkonsekvenser av verktøy som kjøpes inn. Kommunen skal ha oversikt over hvilke personopplysninger som behandles i løsningene, og sikre at ikke opplysningene viderebehandles til nye og uforenelige formål.

---

21 Personvernforordningen artikkel 6 nr. 1 bokstav c. Behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige.

22 Personvernforordningen artikkel 6 nr. 1 bokstav e. Behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt.

23 Lov 17. juni 2005 nr. 64 om barnehager (barnehageloven).

24 Lov 17. juli 1998 nr. 61 om grunnskolen og den vidaregåande opplæringa (opplæringslova).

25 Lov 4. juli 2003 nr. 84 om private skolar med rett til statstilskot (privatskolelova). Se også Lov 10. juni 2022 nr. 39 om endringer i friskolelova (nytt navn på loven og oppheving av to godkjenningsgrunnlag).

26 Prop. 145 L (2020–2021) *Endringar i opplæringslova, friskulelova og barnehagelova (behandling av personopplysningar, fjernundervisning o.a.)* side 5.

27 Prop. 145 L (2020–2021) side 109.

28 Prop. 145 L (2020–2021).

29 Se Opplæringslova § 13-1, For private skoler og barnehager er vil det ofte være selve barnehage- eller skoleledelsen som ansees som skoleeiere.

30 Kunnskapsdepartementet. (2020). *Handlingsplan for digitalisering i grunnopplæringen 2020–2021.*

31 Forskrift 16. oktober 2020 nr. 2063 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften).

Kommunen har ansvaret for at skolen har nettverk, servere og systemer av god nok kvalitet og kapasitet slik at disse støtter opp under både nasjonale og lokale mål for opplæringen, og at elevenes personvern er sikret. Ansvaret ligger hos kommunen, uavhengig av om skolene står for innkjøpene eller om elevene har mulighet til å koble sine egne enheter til skolens nettverk og tjenester.

Kommunen er også ansvarlig for å sikre at barnehagene, skolene og deres ansatte har tilstrekkelig kompetanse til å ivareta elevenes personvern og å sikre «kompetansen som trengs for å undervise og inkludere digitale tema og ressurser i opplæringen».[32]

Kommunen har ansvaret for å ivareta barnas informasjonssikkerhet og personvern når personopplysninger behandles i skolesammenheng. Foreldrene har på sin side ansvar for å ivareta barnas beste, herunder barnas personvern i forbindelse med bruk av digitale enheter utenfor skolen og barnehagen.[33]

Med den økende bruken av digitale læringsverktøy og innlevering av oppgaver og lekser på nett, er likevel skillet mellom skole og fritid mindre skarpt. Barna får tildelt egne nettbrett i undervisning, på samme måte som ansatte får tildelt utstyr fra sine arbeidsgivere. Utfordringer knyttet til dette diskuteres nærmere i avsnitt 8.4.2.

8.3.1.1 Tilsyn i skolesektoren

Utdanningsdirektoratet, statsforvalterne og kommunene kontrollerer om barnehager og skoler følger regelverket ved å gjennomføre tilsyn. Videre fører statsforvalterne tilsyn med offentlige skoler[34] og departementet fører tilsyn med friskoler og private skoler.[35] I tillegg til dette er det kommunen som gjennomfører tilsyn med både kommunale og private barnehager.[36] Det er statsforvalteren som fører tilsyn med kommunene som *skole- og barnehageeier*.[37]

Tilsynene gjennomføres for å kontrollere etterlevelse av opplæringsloven, friskoleloven, barnehageloven og kommuneloven. Hvordan kommunen, skolen eller barnehagen behandler personopplysninger i henhold til personvernregelverket er ikke en del av dette tilsynet, da det faller under Datatilsynets mandat. Datatilsynets tilsynsrolle diskuteres nærmere i kapittel 13.

8.3.2 Barnehageloven og opplæringslova

Barnehageloven regulerer barnehageeier og den enkelte barnehages oppgaver. Lovens kapittel 1 og forskrift om rammeplan for barnehager[38] regulerer overordnet formål i loven og barnehagehverdagens innhold og gir dermed rammene for behandling av personopplysninger i barnehagen.[39] I tillegg gir barnehageloven rettslig grunnlag for behandling av personopplysninger for administrative formål som hører til drift av barnehagene, eksempelvis tildeling av barnehageplass og samarbeid mellom barnehage og foreldre, og andre etater.[40]

Barnehageloven regulerer også mer spesifikt deling av personopplysninger med andre virksomheter. Utgangspunktet er taushetsplikt i henhold til forvaltningsloven.[41] Barnehageloven hjemler når barnehagen har opplysningsplikt til sosial- og helsetjeneste og barnevernet.[42] Videre reguleres deling av personopplysninger mellom barnehagen og skolen i sammenheng med barnets overgang fra barnehage til skole. Deling etter loven kan kun skje med foreldres samtykke.[43] Barnehageloven § 47a annet ledd regulerer barnehagenes muligheter for å dele personopplysninger med ny barnehage dersom barnet skal bytte barnehage. Også her forutsettes at foreldrene samtykker.

Opplæringslova regulerer skoleeier og den enkelte skole sine oppgaver i grunnopplæringen, og gjelder grunnskolen, videregående skole og voksenopplæring. Kapittel 1 i loven angir det overordnede formålet med opplæringen. Dette utgjør rammene for hvilke formål behandlingen av personopplysninger skal skje innenfor ved opplæringen. I tillegg er opplæringslova rettslig grunnlag for de administrative oppgavene som må gjennomføres for å oppfylle kravene i loven, som eksempelvis overgang mellom ulike skoler, sikre oppfølging barna har rett på og generelle administrative oppgaver for drift av skolen.

---

32 Barne- og familiedepartementet. (2021). *Rett på nett. Nasjonal strategi for trygg digital oppvekst.*

33 Utdanningsdirektoratet. (2019). *Hvordan beskytte barn mot skadelig innhold på nett?*

34 Opplæringslova § 14-1.

35 Privatskolelova § 7-2.

36 Barnehageloven § 53.

37 Kommuneloven § 30-2.

38 Forskrift om rammeplan for barnehagens innhold og oppgaver av 24. april 2017 nr. 487.

39 Se blant annet forskrift 24. april 2017 nr 487 om rammeplan for barnehager, kapittel 8 om Barnehagens digitale praksis.

40 Se eksempelvis barnehageloven kapittel IV.

41 Se barnehageloven § 44, jf. forvaltningsloven §§ 13-13g.

42 Se henholdsvis barnehageloven §§ 44 – 46 og 50.

43 Se barnehageloven § 2a.

Opplæringslova regulerer også spesifikt deling av personopplysninger. På samme måte som etter barnehageloven reguleres taushetsplikten i opplæringslova med henvisning til forvaltningsloven.[44] Opplæringslova gir regler for når skolene kan dele personopplysninger til barnevernet, sosial- og helsetjenesten.[45] Lovens § 15-10 annet ledd regulerer skolenes mulighet til å dele personopplysninger med ny skole, ved skolebytte generelt, og ved overgangen fra grunnskole til videregående skole. Delingen av personopplysninger ved skolebytte er ytterligere regulert i forskrift til loven.

8.3.3 Bruk av samtykke

Som nevnt i kapittel 4 må det foreligge rettslig grunnlag for behandling av personopplysninger. Utover det rettslige grunnlaget som nevnt i avsnitt 4.2.7, det vil si at behandlingen er nødvendig for å oppfylle en rettslig forpliktelse eller for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet, kan behandling av personopplysninger på visse vilkår baseres på samtykke. Et samtykke kan kun benyttes som behandlingsgrunnlag dersom det er gitt frivillig.

Et samtykke ansees ikke som frivillig dersom balanseforholdet mellom den registrerte og den behandlingsansvarlige er skjevt. Dersom skjevheten er klar nok, vil det være lite sannsynlig at et samtykke blir «frivillig» avgitt.[46] Personvernforordningen gir ikke eksplisitt uttrykk for hvilket forhold som må foreligge mellom partene for at en skjevhet kan påvirke et samtykke, men Personvernrådet viser særlig til tilfeller hvor det foreligger en klar ubalanse i maktforholdet mellom partene.[47] Dette vil blant annet være tilfelle der den behandlingsansvarlige er en offentlig myndighet eller i forholdet mellom arbeidsgiver og arbeidstaker.[48] Samtykke er derfor mindre egnet som behandlingsgrunnlag for behandling av personopplysninger ved utøving av offentlig myndighet.

For enkelte typer behandlinger i barnehage og skole, vil samtykke likevel være egnet som behandlingsgrunnlag, ifølge forarbeidene til barnehageloven og opplæring- og friskolelova. I forarbeidene nevnes for eksempel at samtykke vil kunne være egnet «ved fotografering av barn/elevar til bruk i skulekatalogar eller ved bruk av ulike appar som fungerer som kommunikasjonsplattform mellom barnehagen/skulen og heimen».[49] Dersom samtykke skal kunne brukes i slike tilfeller, må det sikres at vilkårene for samtykket er oppfylt, det vil si at det er frivillig, informert og utvetydig.[50] Dette betyr at det er avgjørende at skolen eller barnehagen gir tilstrekkelig informasjon om hvilke personopplysninger som skal behandles og hvordan, på en måte som er forståelig for barnet og/eller den foresatte. For at samtykket skal være frivillig, skal det ikke føre til negative konsekvenser dersom man ikke samtykker, for eksempel må ikke manglende samtykke føre til dårligere tjenester eller negativt sosialt press. Styrkeforholdet mellom partene må også tas inn i vurderingen.

8.4 Personvernutfordringer i skole og barnehage i dag

Personvernkommisjonen mener at digitalisering av norsk skole og barnehage har skjedd svært raskt, uten at roller og ansvar for personvernarbeidet, eller konsekvenser for barns personvern er drøftet i tilfredsstillende grad. Ivaretagelse av personvern krever betydelig kompetanse og forståelse for ofte vanskelige juridiske og teknologiske problemstillinger, samt kontinuerlig oppfølging.

I det følgende vil *Personvernkommisjonen* trekke frem de mest sentrale utfordringene knyttet til ivaretakelse av elevers og barns personvern i skolen og barnehagen. Utfordringene henger sammen og er til dels overlappende. Hovedutfordringen er, slik *Personvernkommisjonen* ser det, at kommunene i svært varierende grad har ressurser og kompetanse til å ivareta ansvaret de har etter personvernforordningen for elevenes personvern. Sentrale føringer og veiledning i hvordan elevenes personvern skal ivaretas på best mulig måte, kunne bidratt til å avhjelpe situasjonen kommunene står i. Slike sentrale føringer mangler i dag.

Mangel på tilstrekkelige sentrale føringer, i kombinasjon med varierende grad av kompetanse og ressurser ute i kommunene, medfører også en risiko for at tjenesteleverandører kan legge premissene for hvordan elevenes personvern ivaretas i skolen.

---

44 Se Opplæringslova § 15-1, jf. forvaltningslova §§ 13-13g.

45 Se Opplæringslova kapittel 15.

46 Personvernforordningens fortalepunkt 43 første punktum.

47 European Data Protection Board, Guidelines 5/2020 on consent under Regulation 2016/679, 4. mai 2020, 3.1.1.

48 European Data Protection Board, Guidelines 5/2020 on consent under Regulation 2016/679, 4. mai 2020, avsnitt 16 og 21.

49 Prop. 145 L (2020–2021) *Endringar i opplæringslova, friskulelova og barnehagelova (behandling av personopplysningar, fjernundervisning o.a.)*, avsnitt 2.2.2.2.

50 Se personvernforordningen artikkel 6 første ledd, bokstav a.

8.4.1 Nasjonale føringer

Fra innspillsrunder med aktører i skolesektoren, har *Personvernkommisjonen* fått inntrykk av at det råder usikkerhet om nøyaktig hvilke forpliktelser og oppgaver som påhviler statlige myndigheter og hvilke som påhviler kommunene og den enkelte skole, ved innkjøp og bruk av digitale verktøy. *Kommisjonen* erfarer at aktører i skolesektoren opplever at det er uklart hva behandlingsansvaret innebærer og at ivaretakelse av elevenes personvern mangler en helhetlig og omforent tilnærming.

Representanter fra flere kommuner har spilt inn til *Personvernkommisjonen* at de ønsker mer sentral styring på personvernarbeidet i skole- og barnehagesektoren. *Kommisjonen* har inntrykk av at kommunene ønsker seg, og har behov for, mer praktisk rettet veiledning fra nasjonale myndigheter. Leverandører av digitale skole- og barnehagetjenester har også gitt uttrykk for at de ønsker mer konkret veiledning fra nasjonale myndigheter om hvilke krav som stilles til leverandørene.

Nasjonal handlingsplan for digitalisering i grunnopplæringen, omtalt i avsnitt 8.1.2, inneholder en rekke tiltak for å bedre veiledningen om personvern ut mot skolesektoren.[51] I handlingsplanen nevnes det at videreutvikling av Feide er et viktig tiltak, blant annet for å styrke personvernet. Videre i handlingsplanen foreslås det å utvikle en nasjonal tjenestekatalog for digitale læremidler, for å gi bedre oversikt over hvilke ressurser som finnes, og gi lærerne bedre muligheter til å vurdere styrker og kvaliteter ved disse.

Ifølge tildelingsbrevet for 2021 skal Utdanningsdirektoratet lage veiledning for hvilke krav som bør stilles til leverandører når det gjelder informasjonssikkerhet og personvern. I februar 2022 lanserte Utdanningsdirektoratet en kompetansepakke om personvern i barnehagen – for barnehageeiere, styrere og de som jobber i barnehagen. Utdanningsdirektoratet arbeider også med en kompetansepakke for å øke skoleeiers, skoleledelsens og læreres kompetanse på personvern, som etter det *Personvernkommisjonen* er kjent med, skal være klar mot slutten av 2022.

Personvernkommisjonen mener tiltakene i den nasjonale handlingsplanen er gode og at de potensielt vil kunne møte noe av informasjons- og veiledningsbehovet som finnes ute i kommunene. Det er imidlertid *Personvernkommisjonens* vurdering at selv om flere av tiltakene er positive, så mangler det en tilstrekkelig helhetlig og tydelig styring med hvordan personvernet ivaretas i norske skoler og barnehager.

Det finnes flere måter å innrette den nasjonale styringen på. Den nasjonale styringen kan skje gjennom å etablere en personvernpolitikk for skole- og barnehagesektoren, men også gjennom normarbeid og sentraliserte ordninger som den

[51] Kunnskapsdepartementet. (2017). *Framtid, fornyelse og digitalisering. Digitaliseringsstrategi for grunnopplæringen 2017–2021.*

Boks 8.2 Feide: Innloggingsløsning, ikke godkjenningsordning

Feide er den nasjonale fellesløsningen for pålogging og tilgang. Løsningen leveres av Sikt – Kunnskapssektorens tjenesteleverandør. Sikt samarbeider med Utdanningsdirektoratet om forvaltningen av Feide.

Svært mange av de digitale læremidlene og tjenestene som er i bruk i norsk utdanning benytter Feide som innloggingsløsning. Med en Feide-bruker benytter elever, studenter, forskere og undervisere ett og samme brukernavn og passord til å logge inn på alle tjenester som benytter Feide som innloggingsløsning. Feide er i bruk helt ned til første klasse.

Feide er en sentralisert støtteressurs og løsning, men det er ikke en godkjenningsordning. Det finnes i dag ingen nasjonal godkjenningsordning for læremidler i grunnopplæringen. Det er skoleeierne som har ansvaret for at læremidlene oppfyller kravene til personvern, og at utvalget og kvaliteten er tilstrekkelig til å gi god opplæring.

Ekspertutvalget for læringsanalyse skriver i sin rapport at det er tydelig fra innspillene de har mottatt, at det å inngå i sentraliserte ordninger for læremidler til en viss grad betraktes som et godkjentstempel blant mange skoleeiere, skoleledere, lærere, elever og foresatte. For eksempel er det mange som uttrykker en forventning om høy kvalitet til læremidler med Feide-pålogging.[1]

[1] Kunnskapsdepartementet. (2022). *Læringsanalyse – noen sentrale dilemmaer. Delrapport fra ekspertgruppen for digital læringsanalyse.*

allerede foreslåtte etablering av en tjenestekatalog for digitale læringsmidler.

8.4.1.1 Personvernpolitikk i skole- og barnehagesektoren

Personvernkommisjonen mener det må etableres en helhetlig og offensiv statlig personvernpolitikk i skole- og barnehagesektoren. Per i dag er slik politikk nærmest ikke-eksisterende. Skole og barnehage er der barn og unge læres opp, og det er avgjørende at det offentlige går foran med gode eksempler hva angår grunnleggende verdier som personvern. *Personvernkommisjonen* mener at den nasjonale personvernpolitikken for barnehage og skole må:

- sette kommuner, skoler og barnehager i stand til å bruke digitale tjenester og læringsverktøy på en måte som ivaretar barns og unges personvern.
- sørge for at både barns rett til utdanning og rett til vern av personopplysninger ivaretas, samtidig som kommunalt selvstyre og metodefrihet i skolen og barnehagen bevares.
- stille tydelige krav til kvaliteten på de digitale tjenestene også hva angår personvern. Det er et lovkrav at personvern alltid vurderes og vektlegges ved innføring av nye læringsmidler. Politikken må sørge for at lovkravet følges opp i praksis.
- inneholde og konkretisere krav til at leverandører av tjenester til skole- og barnehagesektoren ikke kan benytte forretningsmodeller som profitterer kommersielt på barns personopplysninger. I praksis betyr dette at det ikke er akseptabelt å benytte leverandører som forbeholder seg retten til å bruke barn og unges data til kommersielle formål, spesielt markedsføringsaktiviteter.
- fange opp tiltak som kommer frem i arbeidet til Ekspertutvalget som er nedsatt for å se på personvernutfordringer knyttet til bruk av læringsanalyse.

8.4.1.2 Nasjonal tjenestekatalog

Kunnskapsdepartementet har gitt Utdanningsdirektoratet i oppdrag å utrede en pilot for en nasjonal tjenestekatalog for digitale læringsmidler.

Utdanningsdirektoratet har startet utredningsarbeidet og i dette arbeidet inngår det å kartlegge hvilken funksjonalitet tjenestekatalogen skal inneholde, utover å gi en samlet oversikt over digitale læringsmidler. Utdanningsdirektoratet oppgir at slik funksjonalitet for eksempel kan være at en kommune kan legge inn informasjon om hvilke læremidler i katalogen som kommunen har kjøpt, har inngått databehandleravtale med og har gjennomført risiko- og sårbarhetsanalyse og personvernkonsekvensvurderinger av. *Personvernkommisjonen* ser dette som en positiv utvikling, da tjenester som tilbys gjennom det offentlige bør ha undergått en viss kvalitetssikring, også av personvern.

Personvernkommisjonen mener behovet for en nasjonal tjenestekatalog er stort. En tjenestekatalog kan være et viktig initiativ for i praksis å sørge for at skoleeiere kan velge tjenester som ikke bare er funksjonelle, men som også ivaretar personvern på en tilfredsstillende måte. Det må sikres at tjenestekatalogen stiller klare og etterprøvbare krav til personvern og informasjonssikkerhet.[52] Tjenestekatalogen bør gi oversikt over læremidler der det er gjennomført risiko- og sårbarhetsanalyse og personvernkonsekvensvurderinger. En velfungerende tjenestekatalog forutsetter kontinuerlige endringer og oppdateringer, da digitale tjenester kan endres fortløpende. Vurderinger fra det nasjonale test- og kompetansemiljøet, som beskrevet i avsnitt 8.4.2, kan inngå i katalogen.

Med tanke på kommunalt selvstyre må det ikke være obligatorisk å benytte læremidler i tjenestekatalogen.[53] *Personvernkommisjonen* understreker at skoleeier i alle tilfeller vil være behandlingsansvarlig og må gjøre egne personvernkonsekvensvurderinger, uavhengig av om en tjeneste inngår i tjenestekatalogen.

8.4.1.3 Personvernnorm for skolesektoren

Det er etter hvert etablert flere bransjenormer for informasjonssikkerhet og personvern innenfor ulike sektorer i Norge. Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) er Norges første og største bransjenorm som gjelder for de aller fleste virksomhetene i helse- og omsorgssektoren.[54] Formålet med Normen er å sikre at opplysninger behandles på en slik måte at helse- og omsorgstjenester kan tilbys på en forsvarlig måte og samtidig ivaretar innbyggernes tillit til sektoren. Ifølge Styringsgruppen til Normen er den særlig viktig fordi den:[55] [56]

---

[52] Kunnskapsdepartementet. (2020). *Handlingsplan for digitalisering i grunnopplæringen 2020–2021.*

[53] Kommuner som unnlater å bruke en slik katalog, og som gjør feil som de kunne ha unngått ved å bruke katalogen, kan imidlertid bli rettslig vurdert ut ifra unnlatelsen.

[54] Direktoratet for e-helse. (2020). *Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.*

- Gjør det enklere å få på plass nødvendige sikkerhets- og personverntiltak
- Bidrar til økt tillit til at sektoren behandler helse- og personopplysninger på en trygg måte
- Bidrar til et harmonisert sikkerhetsnivå i sektoren
- Bidrar til at sektoren har et godt kravstillingsverktøy til informasjonssikkerhet og personvern ved anskaffelser

I barnehage- og skolesektoren behandles det, i likhet med i helsesektoren, store mengder opplysninger. Skolesektoren er videre i likhet med helsesektoren gjenstand for rask digitalisering og den består av aktører med ulik størrelse og med ulik tilgang på ressurser og kompetanse på personvernområdet. I helse- og omsorgssektoren har Normen vært viktig for å få økt oppmerksomhet og ledelsesforankring på personvern. Som trukket frem av styringsgruppen til Normen, er Normen viktig fordi den gjør det enklere å få på plass nødvendige og harmoniserte tiltak. Skolesektoren har mange av de samme utfordringene og behovene som helsesektoren, og *Personvernkommisjonen* mener at etablering av en personvernnorm i skolesektoren, på samme måte som i helsesektoren, kan bidra til å øke oppmerksomheten og ledelsesforankringen på arbeidet med personvern.

Personvernkommisjonen mener statlige myndigheter må ta initiativ til å utarbeide en personvernnorm for skole- og barnehagesektoren. En personvernnorm kan bidra til å sette kommunene bedre i stand til å ivareta behandlingsansvaret sitt og sikre en mer helhetlig og omforent ivaretakelse av barns personvern i barnehagen og grunnskolen. En norm kan også bidra til å forenkle kommunenes anskaffelsesprosesser ved å oppstille krav som leverandørene må etterleve og vil være kjent med.

8.4.2 Kompetanse og ressurser

Kommunene har som behandlingsansvarlig plikt til å skaffe den kompetansen som er nødvendig for å etterleve personvernregelverket. I praksis viser dette seg å være vanskelig for mange kommuner. Det er stor variasjon mellom kommunene når det gjelder tilgang til personvernkompetanse. Små kommuner har ofte få eller ingen dedikerte personvernressurser, mens større kommuner kan ha egne personvernteam med flere ansatte. Alle kommuner skal ha et personvernombud, men også her er det store variasjoner i hvordan kommunene har løst organiseringen av denne funksjonen. Datatilsynets personvernombudundersøkelse viser at mange kommuner har personvernombud ansatt på deltid eller at de deler personvernombud med flere andre kommuner. Mange personvernombud i kommunene er alene om å håndtere personvernspørsmål og har ikke andre personvernressurser eller teknologikompetanse i kommunen å støtte seg på.[57]

Uavhengig av størrelsen på kommunen, har kommunene de samme forpliktelsene til blant annet å gjennomføre risikovurderinger og testing av nye læringsmidler før de kjøpes inn. Manglende tilgang på kompetanse gjør det krevende å følge opp disse forpliktelsene. Gjennomføring av blant annet risikovurderinger er tidkrevende og krever god kompetanse både på juridiske og tekniske forhold.

I praksis har *Personvernkommisjonen* sett at manglende kompetanse får uheldige utslag, for eksempel ved at det mangler retningslinjer for innføring og bruk av apper og hjelpemidler som samler personopplysninger i omfattende grad. Derimot foreligger for eksempel retningslinjer som forhindrer deling av klasselister fordi kommuner og skoler er bekymret for å bryte personvernregelverket. Dette på tross av at Datatilsynet har vurdert at klasselister kan deles, fordi det er viktig for at elever skal kunne møtes, og at alle blir invitert til tilstelninger som bursdager. Forutsetningen er at det er rutiner på plass for å fjerne opplysninger om hemmelig kontaktinformasjon.

I Bouvets rapport «Digitalisering i skolen. Har vi glemt personvernet?», fremkommer det fra intervjuer med aktører i skolen at det å gjennomføre en ROS-analyse av en læringsressurs tar minst fem timer og at to personer bør involveres.[58] Med tanke på alle de ulike fagene i skolen som krever ulike læringsmidler, fordelt over klassetrinn med ulikt læringsbehov, blir det en svært arbeidskrevende jobb å risikovurdere alle løsningene som ønskes innført. Intervjuobjektene i Bouvets rapport gir tydelig tilbakemelding på at de verken har kapasitet eller kompetanse til å håndtere mengden av alle vurderinger som må gjøres.

---

55 Direktoratet for e-helse. (2019). *Strategi for Normen, 2019–2020.*

56 Normen anses å være et veiledende dokument og har ikke status som atferdsnorm etter personvernforordningen art. 40.

57 Datatilsynet. (2020). *Personvernombudsundersøkelsen 2020/21.*

58 Bouvet. (2021). *Digitalisering i skolen. Har vi glemt personvernet?*

IT-leverandørene oppdaterer ofte i tillegg tjenestene og vilkårene underveis i avtaleforholdet. For kommunene kreves det dermed ikke kun ressurser til å gjennomføre risikoanalyser og inngå avtaler med leverandørene, men også til å *følge opp* løsningen over tid og påse at personvernet ivaretas når det gjøres endringer i løsningen. Dersom en leverandør endrer en tjeneste på en måte som utfordrer personvernet, stilles kommunen i en vanskelig posisjon. Enten må kommunene forsøke å forhandle med leverandøren, eller bytte system, som krever mye ressurser og tid.

Den store variasjonen i tilgang på personvernkompetanse fører til store forskjeller mellom kommunene i hvordan personvernregelverket blir etterlevd og dermed i hvilken grad personvernet til barna i skolen og barnehagen blir ivaretatt. Det fører også til forskjeller i hvilke læringsmidler store og små kommuner har ressurser til å vurdere og dermed til å ta i bruk. Ulik tilgang på personvernkompetanse påvirker altså ikke bare personvernet, men også hvilke digitale læringsmidler og pedagogiske løsninger elevene i ulike kommuner har tilgang til.

Som et svar på kompetanse- og ressursutfordringene i skolesektoren knyttet til ivaretakelse av personvern, etablerte KS prosjektet *Skolesec* i 2021. Formålet med Skolesec er å se på muligheter for forenkling og forbedring av personvern- og informasjonssikkerhetsprosesser i anskaffelse og implementering av digitale tjenester i skolen. Prosjektet har fått midler til å drive ut 2022.

Personvernkommisjonen mener det er avgjørende for personvernet til barn i skole og barnehage at kommunene sikres tilstrekkelige personvernressurser, herunder tilgang på ressurser med grunnleggende teknologikompetanse. Dette er en forutsetning for å kunne gjøre gode vurderinger og ivareta personvernet på løpende basis.

Personvernkommisjonen mener det må etableres mekanismer som legger til rette for at kommunene kan ivareta behandlingsansvaret på en bedre måte enn i dag. Risikovurderinger og testing av digitale løsninger som skal brukes i skoler og barnehager over hele landet, bør profesjonaliseres og sentraliseres.

Personvernkommisjonen anbefaler at det etableres, eller videreutvikles i allerede eksisterende strukturer (som Skolesec eller Sikt), et tverrfaglig nasjonalt test- og kompetansemilø som ivaretar følgende funksjoner:

- *Kompetansemiljø som koordinerer og utvikler verktøy og malverk* som setter kommunene i stand til å gjennomføre risikovurderinger og personvernkonsekvensvurderinger og å etablere effektiv internkontroll.
- *Testing* av digitale løsninger som skal brukes i skoler og barnehager. Resultatene fra testingen av løsningene bør kommuniseres videre til de ansvarlige for den nasjonale tjenestekatalogen.
- *Forhandlingsledelse og forhandlingsstøtte* til kommunene i deres forhandlinger med plattformleverandørene. Dette vil styrke kommunenes forhandlingsmakt ved at det vil være lettere å stille nødvendige krav til tjenestene (utfordringer knyttet til innkjøp og forhandlinger er nærmere diskutert avsnitt 8.4.5)

For å sikre at hver enkelt kommune ivaretar ansvaret som behandlingsansvarlig for løsningene, er det viktig å påse at kommunene etablerer rutiner for systematiske risikovurderinger av løsningene etter at de er implementert.

8.4.3 Ansvar og rutiner

Å implementere gode rutiner, med tydelige beskrivelser av roller og ansvar, er viktig for å sikre etterlevelse av personvernregelverket. Dette er særlig viktig i skole- og barnehagesektoren, fordi det ofte er lang avstand mellom kommunen som behandlingsansvarlig og ned til skole- og barnehagehverdagen, der de digitale læringsmidlene tas i bruk og behovet for anskaffelser av nye læringsmidler oppstår.

Det er viktig at kommunen og skolen samarbeider godt om å ivareta elevenes personvern. Kommunen skal blant annet gjennomføre organisatoriske tiltak for å sikre etterlevelse av personvernregelverket.[59] For eksempel kan ansvaret utøves av rektor. Uansett er det kommunens øverste ledelse som har ansvaret for behandlingen.

Gode internkontrollrutiner, med tydelig beskrivelse av roller og ansvar, skal sikre at alle fra kommunenivå og ned til skoleledelsen og den enkelte ansatte, kjenner til pliktene i personvernregelverket og hvordan de skal gå frem for å ivareta personvernet til elevene og barnehagebarna. Uten gode rutiner er det krevende for kommunen å ivareta sitt behandlingsansvar.

Kommisjonen har etter innspillsrunder med representanter fra kommunene fått inntrykk av at det er utfordrende å etablere gode rutiner for personvernarbeidet. Kommunen har gjerne overordnede rutiner for internkontroll, men disse er ofte lite kjent i barnehagene og skolene. Rutinene er

[59] Personvernforordningen art. 24 nr. 1.

Boks 8.3 Bot til Ålesund kommune for bruk av treningsappen Strava

Lærere i Ålesund kommune påla elever å laste ned treningsappen Strava på deres private mobiltelefoner. Appen ble brukt av elevene til å utføre oppgaver og ble brukt av lærerne til å sjekke om elevene hadde gjennomført, ved hjelp av sporing.

Datatilsynet konkluderte med at det forelå et brudd på personvernforordningen artikkel 24 nr. 1, for ikke å ha etablert rutiner for tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen. Videre mente Datatilsynet at det ikke var gjennomført en risikovurdering som kreves i tråd med artikkel 32. Datatilsynet kom til slutt til at behandling av elevenes personopplysninger i appen medførte høy risiko for elevenes rettigheter og friheter. En personvernkonsekvensvurdering var dermed nødvendig, i tråd med personvernforordningen artikkel 35.

Datatilsynet ila Ålesund kommune et overtredelsesgebyr på 50 000 kroner. Datatilsynet la blant annet vekt på at appen ble lastet ned på elevenes private mobiler og at Ålesund kommune «burde vært rustet» til å ivareta personvernforordningens krav. Overtredelsesgebyret ble også begrunnet med at et slikt vedtak gir en «viktig signaleffekt».[1]

[1] Datatilsynet (2021, 23. mars). *Gebyr til Ålesund kommune for bruk av Strava*

ofte heller ikke tilpasset skole- og barnehagesektorens særskilte utfordringer. Dette fører blant annet til at lærere eller barnehagelærere tar i bruk digitale verktøy uten at det rapporteres videre til skolens eller barnehagens ledelse, eller fra skoleledelsen og videre opp til skoleeier.

Personvernkommisjonen har for eksempel inntrykk av at det ikke er uvanlig at det er lærerne som velger ut hvilke «gratisverktøy» de ønsker å benytte seg av i undervisningen og at gratisapper benyttes i noe grad for å bøte på manglende ressurser til å betale for læringsverktøy. Disse verktøyene går ikke gjennom kommunens anskaffelsesbudsjett og det foretas ofte ikke vurderinger av personvernrisiko før verktøyet tas i bruk.

Ålesund kommune ble ilagt overtredelsesgebyr fra Datatilsynet i 2021 etter at lærere ved en skole påla elevene å laste ned treningsappen Strava på deres private mobiltelefoner. Saken illustrerer viktigheten av å ha gode rutiner og opplæring, for å sikre at alle som er involvert i bestilling og bruk av digitale verktøy i skolen vet hvem som har ansvaret for å gjøre hva, før løsninger tas i bruk.

Personvernkommisjonen mener kommunene som behandlingsansvarlig i større grad må utarbeide tilpassede rutiner og veiledning til skoleledelse og lærere. Det bør blant annet utarbeides retningslinjer som klargjør roller og ansvar knyttet til anskaffelse og bruk av nye digitale læringsverktøy. Rutiner som er tilpasset de enkelte situasjonene vil i større grad sikre at regelverket etterleves og gir samtidig de ansatte i skolen en større trygghet om at det de gjør er riktig.

Personvernkommisjonen mener Utdanningsdirektoratet i større grad bør hjelpe og tilrettelegge for at kommunene kan ivareta sitt behandlingsansvar etter personvernregelverket. Dette innebærer blant annet at kommunene får bistand til å etablere nødvendige og tilpassede rutiner samt veiledning.

8.4.3.1 Rutiner for bruk av skolens digitale læringsmidler utenfor skolen

Som omtalt i avsnitt 8.3 om rettslige rammer, har kommunen ansvar for å ivareta barns informasjonssikkerhet og personvern når personopplysninger behandles i skolesammenheng. Foreldrene har på sin side ansvar for å ivareta barns beste, herunder barns personvern, i forbindelse med bruk av digitale enheter utenfor skolen og barnehagen.

Med den økende bruken av digitale læringsverktøy og innlevering av oppgaver og lekser på nett, har skillet mellom skole og fritid blitt mindre skarpt. Ved mange skoler får elevene tildelt egne nettbrett av skolen. Enhetene må tas med hjem for å gjøre lekser og kobles til internett utenfor skolens nettverk. Barna har ofte mulighet til også å benytte nettbrettene og PC-ene til private aktiviteter.

I praksis ligger en stor del av ansvaret for ivaretakelse av informasjonssikkerhet og personvern hos skolen, fremfor foreldre/foresatte. Skolen har

administratorrettigheter til utstyret, og er de eneste som har mulighet til å konfigurere enhetene, slik at personvern er ivaretatt i standardinnstillingene på samtlige enheter. Dette innebærer at skolene eksempelvis kan konfigurere standardinnstillinger for nettleser, innholdsfiltre[60] og andre teknologiske virkemidler for å sikre at elevenes personvern blir ivaretatt på best mulig måte. Det er videre kun administrator som kan velge hvor mye data som automatisk deles med leverandør om bruk av operativsystemet, eller velge hvilken nettleser som er installert på PC-en eller nettbrettet. Foresatte har ikke mulighet til å gå inn og endre innstillinger for å hindre at opplysninger om barnet samles inn av operativsystemet som benyttes.[61]

I sin kartlegging har *Personvernkommisjonen* ikke sett eksempler på skriftlige rutiner som tydeliggjør kommunens ansvar for elevenes personvern ved bruk av skolens digitale utstyr utenfor skolen.

Personvernkommisjonen mener det er viktig at kommunene har rutiner som sikrer at barns personvern ivaretas når digitale verktøy benyttes utenfor skolens område. Dette betyr blant annet å tydeliggjøre eventuelle begrensninger i skolens ansvar, og å utarbeide retningslinjer for hvordan foreldre kan bidra til å ivareta sine barns personvern ved bruk av digitale verktøy utenfor skolen. Endelig bør kommunene regelmessig følge opp og vurdere om tiltakene og rutinene til enhver tid er tilstrekkelige.

Mange av de digitale læringsmidlene elevene benytter til skolearbeid lagrer opplysninger om hvor, når og hvor lenge skolearbeidet ble utført. Dette medfører risiko for at lærere og andre ansatte ved skolen kan benytte disse opplysningene til å føre kontroll med for eksempel når på døgnet lekser utføres og hvor mye tid elevene bruker på skolearbeidet.

Personvernkommisjonen mener det er viktig at kommunene har rutiner og retningslinjer som sikrer at ikke lærere og andre ansatte ved skolen bruker opplysninger som samles inn og lagres i elevenes digitale enheter til kontrollformål. Kommunen må også lage rutiner som påser at elever og foreldre informeres om hvilke opplysninger som samles inn og hva de brukes til. Viktigheten av informasjon diskuteres nærmere i avsnitt 8.4.8

Personvernkommisjonen mener det vil være synergieffekter å hente ut for kommunene hvis de samarbeider med andre kommuner om utarbeidelse av veiledende rutiner. Som behandlingsansvarlig er det også kommunens ansvar å sørge for at ansatte i skolen har tilstrekkelig kompetanse til å ivareta elevenes personvern. Som ledd i arbeidet med å styrke internkontrollen i skole- og barnehagesektoren, mener *kommisjonen* at lærere og barnehagelærere må få bedre opplæring i personvern og hensynene bak personvernregelverket. Hvordan digitale verktøy brukes i praksis har stor betydning for ivaretakelsen av personvernet til barna.

8.4.4 Bruk av elevers personopplysninger til kommersielle formål

Mange av systemene og tjenestene som brukes i skolen leveres av kommersielle aktører som samler inn personopplysninger for analyseformål, levering av tilpassede tjenester, eller for andre kommersielle formål.

Det kan være særskilte utfordringer knyttet til bruken av tjenester for å levere tilpasset læringsanalyse eller for å analysere/måle elevers aktiviteter og prestasjoner, inkludert mulig diskriminering, skjeve resultater og nedkjølingseffekter på elevers atferd. Dette er problemstillinger som Ekspertutvalget for læringsanalyse skal se nærmere på, og vil følgelig ikke behandles videre her.

Problemstillinger knyttet til innsamling og analyse av elevers personopplysninger er relevante også for andre verktøy enn kun læringsanalyseverktøy. Bruken av kommersielle verktøy i skolen innebærer i mange tilfeller at det samles inn personopplysninger til formål utover å levere tjenesten til elevene. Det er skoleeiers ansvar å sørge for at verktøy som tas i bruk ikke bryter med personvernprinsippene.

Det kan være flere årsaker til at skoler tar i bruk kommersielle digitale verktøy, slik som nytteverdi, at elever er vant til grensesnittet, at verktøyene er rimelige eller ikke koster noe å anskaffe, og en rekke andre grunner. Før slike verktøy anskaffes og tas i bruk må det uansett foretas en personvernvurdering for å sikre at elevenes personvern ivaretas.

Datatilsynet peker i sin årsrapport fra 2020 på særlige utfordringer knyttet til bruken av såkalte «gratisapper» i skolen. Tilsynet understreker at bruken av slike verktøy som regel vil innebære at personopplysninger om elevene samles inn og anvendes til andre formål.[62] Selv om bruken av gratistjenester gjerne innebærer at leverandøren har en forretningsmodell basert på bruk av per-

[60] Se blant annet i Utdanningsdirektoratet. (2019). *Hvordan beskytte barn mot skadelig innhold på nett?*

[61] Se blant annet i Utdanningsdirektoratet. (2019). *Hvordan beskytte barn mot skadelig innhold på nett?*

[62] Datatilsynet. (2020). *Årsrapport for 2020.*

Boks 8.4 Bruk av digital læringsanalyse innebærer personvernutfordringer

Prosjektet «Aktivitetsdata for vurdering og tilpassing» er et forsknings- og utviklingsprosjekt som skal se på utfordringer og muligheter ved bruk av læringsanalyse og kunstig intelligens for å analysere aktivitetsdata om elever fra digitale læremidler. Prosjektet var en del av Datatilsynets sandkasse for kunstig intelligens. I sin sluttrapport om sandkasseprosjektet peker Datatilsynet på at anvendelsen av slike verktøy innebærer personvernrisiko, særlig knyttet til nedkjølingseffekter, uriktige personopplysninger i systemet, samt at systemet kan påføre elever unødvendig stress. Tilsynet beskriver også mulig risiko knyttet til særlige kategorier av personopplysninger, tredjeparters behandling av opplysningene, samt at systemet har grensedragninger mot et automatisk beslutningssystem.[1]

[1] Datatilsynet. (2022). *ATV. Sluttrapport fra sandkasseprosjektet med KS, SLATE ved UiB og Utdanningsetaten i Oslo kommune.*

sonopplysninger, betyr ikke dette at betalte alternativer nødvendigvis ikke bruker, deler eller selger personopplysninger.[63]

Som beskrevet nærmere i kapittel 9 om forbrukernes personvern, har det oppstått et stort kommersielt marked for personopplysninger. I tillegg til å anvendes for å levere bedre tjenester, deles personopplysninger med tredjeparter, brukes til markedsføringsformål, profileringsformål og mye mer. I forbrukersammenheng er denne bruken av personopplysninger ofte basert på forbrukerens samtykke – selv om slike samtykker har klare begrensninger. Ved bruk av verktøy i skolen har elevene, eller deres foresatte, som regel ikke noe annet valg enn å ta i bruk tjenestene. Det er skoleeier som dermed må sørge for å ha oversikt over hvordan verktøyene behandler personopplysninger, hvilke tredjeparter opplysningene eventuelt kan deles med, og hvilke formål de kan brukes til.

I praksis er det svært utfordrende for den enkelte skoleeier å ha oversikt over hvordan personopplysninger samles inn og brukes når elever tar i bruk kommersielle verktøy. Det kan føre til at elevenes personopplysninger deles i vid utstrekning. For eksempel avdekket Bouvet i sin rapport om personvern i skolen at tjenester benyttet i skolen deler lokasjonsdata, viderebehandler personopplysninger til uspesifiserte formål, og at elevenes personopplysninger lagres i USA.[64]

Da skoler og barnehager stengte i mars 2020 som følge av covid-19-pandemien, måtte all undervisning foregå digitalt. Lærerne ble oppmuntret av kommunene til å bruke gratis læringsressurser på nett og fikk nyttige erfaringer og mer kunnskap om digitale læringsverktøy. Da skolene ble stengt ned, kom undervisningen i første rekke, mens regler og rutiner om personvern kom på plass etter hvert.[65]

Bruken av Google i skolen reiser også mulige personvernutfordringer. I 2020 irettesatte Datatilsynet tre kommuner for deres bruk av verktøyene Google Chromebook og G Suite for Education.[66] En undersøkelse gjennomført av tilsynet avdekket betydelige mangler ved hvordan kommunene hadde tatt i bruk verktøyene i skolen. Ifølge Datatilsynet inkluderte manglene at kommunene ikke ga informasjon om riktig behandlingsgrunnlag for behandlingen, at de manglet oversikt over hvilke personopplysninger som ble behandlet til hvilke formål, og manglende risikovurderinger.

I kjølvannet av undersøkelsene publiserte Datatilsynet en veileder for bruk av Google Chromebook og G Suite for Education i grunnskolen.[67] Tilsynet anbefaler blant annet at kommuner avstår fra å ta i bruk digitale tjenester som innebærer profilering av elevene. Datatilsynet understreker at kommunene må gjøre en fullstendig gjennomgang av avtalene tjenester de ønsker å benytte er omfattet av. I tillegg til å ha oversikt over databehandlingen og avtalene som regulerer dette, må kommunene gi tilstrekkelig informasjon til elever og foresatte, for å sikre at disse kan ivareta sine rettigheter. Kommunene skal også forsikre seg om at løsningene de vil benytte har innebygd personvern, at det føres protokoll over behandlingsaktivitetene, samt at det gjennomføres grundige

[63] Seneviratne, S., Kola H. & Seneviratne, A. (2015). A measurement study of tracking in paid mobile applications. *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec).*

[64] Bouvet. (2021). *Digitalisering i skolen. Har vi glemt personvernet?*

[65] Bouvet. (2021). *Digitalisering i skolen. Har vi glemt personvernet?*

[66] Datatilsynet. (2020). *Varsel om irettesettelse for feil bruk av Googles løsninger i skolen.*

[67] Datatilsynet. (2020). *Bruk av Google Chromebook og G Suite for Education (og andre skytjenester) i grunnskolen.*

Boks 8.5 Løsninger som utnytter elevopplysninger til kommersielle formål

I 2022 publiserte menneskerettighetsorganisasjonen Human Rights Watch en rapport hvor de gjennomgikk 164 forskjellige læringsverktøy som var blitt anbefalt av myndighetene i 49 land i forbindelse med hjemmeskole under covid-19.[1] Organisasjonen oppdaget at 146 av læringsverktøys-appene som var testet, eller 89 %, syntes å dele eller anvende data på måter som satt barnas rettigheter i fare eller direkte brøt med rettighetene. Funnene inkluderte datainnsamling og -deling om barna, vennene og familiene deres, sporing utenfor klasserommet og rundt på andre nettsteder, og detaljert profilering av barna. Norge var ikke blant landene som ble undersøkt.

[1] Human Rights Watch. (2022). *Students – not products.*

Boks 8.6 Reklame for slanketabletter i skolekalkulator-app]

Som et eksempel på uakseptabel eksponering for markedsføring i apper brukt i skolen, ble *Personvernkommisjonen* gjort oppmerksom på et tilfelle hvor en jente på syvende trinn ble vist annonser for slanketabletter i kalkulator-appen på skolens iPad.

Figur 8.2

Kilde: Far til datter (12 år).

risikovurderinger av personvern og IKT-sikkerhet.

Eksemplene ovenfor illustrerer at det kan være svært vanskelig for den enkelte skoleeier å ha oversikt over hvordan personopplysninger behandles ved bruk av kommersielle verktøy. Brukervilkår og personvernerklæringer er ofte mange, lange og kompliserte. Det er ofte nødvendig med høy personvernkompetanse for å kunne forstå innholdet i vilkårene og erklæringene. Samtidig er digitale verktøy i mange tilfeller sammensatte tjenester, med flere tredje- og fjerdepartsleverandører i verdikjedene, samt at forretningsmodellene er vanskelig å skjønne. For eksempel kan det være vanskelig å fastslå om profilering av elevene skjer og om disse profilene brukes for eksempel til markedsføring, eller om personopplysningene og profilene om eleven faktisk slettes etter en viss tid. Det krever også spesialkompetanse for å etterprøve hvordan personopplysninger behandles og/ eller hvor de overføres. I tillegg kan det være utfordrende å formidle informasjon om behandlingen til elever og foresatte.

Personvernkommisjonen vil imidlertid påpeke at den omfattende kommersielle innsamlingen, behandlingen og delingen av personopplysninger som har blitt normalisert i skolen og barnehagen ikke alene kan løses gjennom å gi foreldre og barn mer informasjon. Det er *kommisjonens* syn at utfordringene knyttet til dagens digitaliserte skole og barnehage ikke lar seg løse ved å overlate ansvaret til foreldre og barn. I stedet må skoleeiere gjennomføre konkrete vurderinger av alle verktøy som benyttes og sørge for at verktøy med omfattende kommersiell sporing ikke benyttes i skolen.

Personvernkommisjonen er også bekymret for at elever, gjennom ukritisk bruk av kommersielle digitale tjenester i skolen, blir opplært til å selv ha et ureflektert forhold til bruk av digitale tjenester. Som beskrevet i kapittel 9 om forbrukernes personvern, kan utstrakt innsamling av personopplysninger føre til personvernkynisme, hvor man gir opp å ivareta eget personvern fordi man overveldes. Det er svært uheldig dersom skolene bidrar til denne utviklingen.

Personvernkommisjonen mener regjeringen må sette av midler og sørge for tilgang til kompetanse for fortløpende evalueringer av hvordan, og i hvilken grad, digitale læremidler påvirker og ivaretar barns personvern.

Personvernkommisjonen mener regjeringen må ta initiativ til en bred utredning av digitale verktøy som er i bruk i norsk skole i dag og hvordan de påvirker barns personvern. En slik utredning bør gjelde alle typer læremidler og øvrige metoder og verktøy som brukes i undervisningssammen-

heng. Hvilke kontroll- og overvåkningsmuligheter disse verktøyene gir, hvilken kunnskap det er mulig å trekke ut av opplysningene som samles inn og lagres og hvordan kunnskapen blir brukt til nytte for elever og for utdanningsinstitusjoner, bør belyses i en slik utredning. Videre bør det kartlegges hvordan personopplysningene som samles inn viderebehandles til ulike formål.

På oppdrag fra *Personvernkommisjonen*, har Christian Falch gjennomført intervjuer med 37 elever fra 8 – 19 år om holdninger til og kunnskap om personvern.[68] Et av funnene i Falchs rapport er at «alle deltakerne i undersøkelsen oppgir at de får mye reklame på læringsbrett og skole-PCer. Her er reklame direkte i apper, i nettlesere og for eksempel i forbindelse med visning av innhold på YouTube noe de fleste trekker frem. Eksponering for reklame er et stort og alvorlig problem i skolehverdagen og bør adresses som et eget tema». *Personvernkommisjonen* vil påpeke at skoleeier har plikt til å skjerme elevene for uønsket påvirkning etter opplæringsloven § 9-6 og privatskoleloven § 7-1a.[69]

Personvernkommisjonen mener annonseblokkeringsverktøy eller andre tiltak på elevenes utstyr må vurderes som et tiltak for å redusere elevenes eksponering mot reklame. Dette kan i tillegg bidra til å redusere sporingen av elevenes digitale aktivitet til kommersielle formål.

8.4.5 Innkjøp og forhandlinger

Det er kommunen som behandlingsansvarlig som har ansvaret for å kjøpe inn digitale løsninger til bruk i skolen. Løsningene som leveres til skolen blir stadig mer komplekse og krever at innkjøperen har god forståelse for de teknologiske, juridiske og forretningsmessige aspektene av tjenestene. Hvis denne kompetansen ikke er på plass, blir leverandørene i praksis premissgiver for hvordan barnas personopplysninger behandles i skolen og barnehagen.

Personvernkommisjonen har i innspillsmøter fått tilbakemelding på at det er store forskjeller i hvilken grad kommunene har kompetanse og ressurser til å ivareta forhandlingsmakten overfor leverandørene. Mange store kommuner har teknologiforståelse, juridisk kunnskap og kapasitet til å sette krav til produktene de kjøper, samt til å gjøre tilpasninger av systemer og bruk, slik at produktet oppfyller kravene til personvern og informasjonssikkerhet. Mange små kommuner, uten samme tilgang til personvernkompetanse, vil derimot i større grad kjøpe IKT-tjenester som hyllevare uten at det settes krav til tilpasninger for å ivareta elevenes personvern.

I handlingsplanen for digitalisering i grunnopplæringen skriver Kunnskapsdepartementet at kommunenes forhandlingsmakt med de internasjonale selskapene Google, Microsoft og Apple er begrenset.[70] Handlingsplanen kommer ikke med anbefalinger eller tiltak til hvordan kommunenes forhandlingsmakt kan styrkes.

I forhandlinger med leverandører, spesielt med de store teknologiselskapene, er det en fordel å selv være en stor aktør for å få gjennomslag for særskilte krav. For å styrke og profesjonalisere innkjøpsmakten sin, har enkelte kommuner gått sammen og sentralisert anskaffelse av digitale enheter og læringsressurser ved å opprette interkommunale selskap. Et eksempel er Søre Sunnmøre IKT som er et interkommunalt selskap eid av sju kommuner i Møre og Romsdal.[71]

Det er ikke nødvendigvis slik at alle digitale verktøy i utdanningssektoren må kjøpes inn fra eksterne leverandører. Som i andre sektorer, for eksempel innen helsesektoren, vil det i visse tilfeller være aktuelt at det offentlige utvikler egne tjenester og verktøy for skole- og barnehagesektoren, som beskrevet nedenfor i avsnitt 8.4.6.

Ettersom det er kommunene som er behandlingsansvarlige og dermed ansvarlige for å gjøre forsvarlige innkjøp av nye løsninger, har ikke staten en rolle som forhandlingspart ved innkjøp av digitale læremidler i skolesektoren. *Personvernkommisjonen* mener likevel at innkjøp og forhandlinger, spesielt fra de store plattformleverandørene, bør profesjonaliseres og sentraliseres. Statlige myndigheter og/eller KS bør gå aktivt inn i forhandlinger med plattformleverandørene på vegne av kommunene for å avhjelpe maktskjevheten mange småkommuner står i. Ved å styrke forhandlingsmakten vil det være lettere å stille nødvendige krav, og få gjennomslag for kravene, til tjenestene som behandler personopplysninger om elever og barnehagebarn. Kommersiell utnytting av personopplysninger i skolen er etter *Personvernkommisjonens* syn ikke akseptabelt.

---

68 *Personvernkommisjonen* ønsket å utføre en kvalitativ undersøkelse om holdninger til og kunnskap om personvern blant barn og unge. Christian Falch har produsert rapporten «Rapport til personvernkommisjonen. Intervjuer med barn og unge om personvern». Rapporten bygger på gruppeintervjuer med 37 barn og unge i alderen 8 – 19 år. Deltakerne er plukket ut med tanke på demografisk og geografisk variasjon. Falch, C. (2022). *Rapport til Personvernkommisjonen. Intervjuer med barn og unge om personvern.*

69 Utdanningsdirektoratet. (2011). *Reklame i skolen - veileder.*

70 Kunnskapsdepartementet. (2020). *Handlingsplan for digitalisering i grunnopplæringen 2020–2021.*

71 Søre Sunnmøre IKT. (2022). *Om SSIKT.*

Boks 8.7 Eksempel på innkjøpssamarbeid

Et eksempel på hvordan staten og Datatilsynet kan samarbeide for å fremme personvernet kommer fra Nederland:

Den nederlandske staten ga et privat konsulentselskap (the Privacy Company) i oppdrag å gjennomføre en personvernkonsekvensutredning for G Suite Enterprise og Google Workspace. Personvernkonsekvensvurderingen avdekket høy risiko for elevenes personvern og staten som behandlingsansvarlig innledet forhandlinger med Google for å få endret standardvilkårene i databehandleravtalen. Siden Google kun i liten grad gjennomførte tekniske og organisatoriske tiltak for å redusere risikoen,[1] innledet staten forhåndsdrøftelser med det nederlandske Datatilsynet i henhold til forordningens artikkel 36. Gjennom denne fremgangsmåten lykkes staten å få Google til å vurdere endringer i standardvilkårene i databehandleravtalen for bruken av tjenesten.[2]

1 Privacy Company. (2021). *Google mitigates 8 high privacy risks for Workspace for Education*.

2 Privacy Company. (2021). *Privacy assessment Google Workspace (G Suite) Enterprise: Dutch government consults Dutch Data Protection Authority on high privacy risks*.

Personvernkommisjonen mener innkjøp og forhandlinger av løsninger til skole- og barnehagesektoren må forankres i den nasjonale personvernpolitikken for skolen og barnehagen. Denne politikken må inneholde tydelige krav til kvaliteten på læringsmidlene, samtidig som de ivaretar barns rett til personvern og vern mot at data som samles inn om elevene benyttes til kommersielle formål.

I avsnitt 8.4.2 foreslår *Personvernkommisjonen* at bistand til forhandlingsledelse og forhandlingsstøtte kan legges til et nasjonalt test- og kompetansemiljø. *Kommisjonen* mener statlige myndigheter bør se på muligheten for å inngå samarbeid med andre land i forhandlinger med de globale plattformleverandørene, for eksempel innenfor rammen av det nordiske samarbeidet.

8.4.6 Utvikling av digitale læringsverktøy

De globale plattformleverandørene har på få år blitt dominerende på leverandørsiden i norsk skole. Disse leverandørene leverer både gode og brukervennlige tjenester til en rimelig pris. Dette harmonerer godt med skoler og barnehagers ambisjoner om å kunne drive god læring med gode verktøy til en pris som passer i deres begrensede budsjetter. Samtidig kan utviklingen skape en uheldig markedsdominans som gjør at personvernvennlige alternativer ikke slipper til på markedet.

Skolesektoren er et attraktivt marked for plattformleverandørene av flere årsaker. For det første tjener leverandørene på ordinær betaling for levering av software og hardware-produkter. Skolen er imidlertid også et attraktivt marked fordi det gjør det mulig for leverandørene å etablere en forbrukerrelasjon til barna, en forbrukerrelasjon som potensielt kan vare livet ut. Barna blir gjennom skolen vant til å bruke et bestemt operativsystem og brukergrensesnitt og terskelen for å bytte tjeneste blir høy. På denne måten er det å tilby svært billige tjenester til skole og barnehage en investering som kan gi betydelige gevinster for selskapene i et lengre perspektiv.

Utenfor skolesystemet er det foreldrene eller barnet selv som velger hvilken tjeneste som skal benyttes. I skolen er det kommunen som er ansvarlig for å velge tjenesteleverandør og hvordan og i hvilket omfang tjenesten skal brukes. Kommuner og skolemyndigheter har dermed stor påvirkningskraft på innbyggernes forhold til digitale tjenester. Det er viktig at kommunene forstår og er bevisst dette ansvaret når de går til innkjøp av digitale tjenester i skolen.

Som beskrevet i kapittel 9 om forbrukernes personvern, kan markedsdominansen til de globale tjenesteleverandørene innenfor digitale tjenester føre til svekket personvern ved at personvernvennlige alternativer ikke klarer å entre markedet. Dette gjelder også i skolesektoren. *Personvernkommisjonen* har hatt dialog med den norske edtechbransjen gjennom leverandøren Neddy, som gir uttrykk for at det i dag er krevende for mindre, nasjonale, aktører å få solgt sine tjenester til skolesektoren.

Personvernkommisjonen mener den nasjonale personvernpolitikken for skole- og barnehagesektoren bør inneholde tiltak for å støtte norske virksomheter som utvikler løsninger som bygger opp under prinsippene i den nasjonale utdanningspolitikken og barns grunnleggende rettigheter – og som ikke bygger på en forretningsmodell som profitterer på barns personopplysninger.

Boks 8.8 Dansk fond for utviklingsstøtte til nasjonale læringsmidler

Fagorganisasjonen Djøf[1] i Danmark har etablert Tech DK Kommission som er en uavhengig kommisjon med medlemmer fra ulike fagområder som vurderer teknologiens rolle i samfunnet. *Kommisjonen* har blant annet publisert rapporten *Uddannelse og tech*. Et av tiltakene som anbefales i rapporten er å etablere et *statlig eid teknologiutdanningsfond* som investerer i utvikling av danske, etisk forsvarlige digitale læringsplattformer og programmer. Målet er å bidra til at det ikke kun er amerikanske eller kinesiske bedrifter, basert på helt andre undervisningskulturer og med kommersielle interesser, som styrer utviklingen av læremidler. Fondet skal dele ut midler til prosjekter som støtter digital undervisning basert på dansk og europeisk utdanningskultur og respekt for brukerens læring, erfaring, databeskyttelse og helse.[2]

1 Djøf er en faglig organisasjon for akademikere og studenter innen samfunnsvitenskap og bedriftsøkonomi. Djøf har ca. 130 000 medlemmer.

2 TechDK Kommissionen. (2020). *Analyse: Uddannelse og tech*.

Personvernkommisjonen mener at dersom vurderinger gjennomført av det nasjonale test- og kompetansesenteret viser at eksisterende løsninger ikke ivaretar personvernet på en tilfredsstillende måte, må statlige myndigheter investere i utvikling av nye, forsvarlige løsninger. *Kommisjonen* anser at det kan være hensiktsmessig å gjøre slike investeringer i europeisk eller nordisk regi. Norge kan, og bør etter *kommisjonens* syn, ta en foregangsrolle i dette arbeidet.

8.4.7 Undervisning i personvern

De siste årene har læreplaner og strategier vektlagt digital kompetanse hos barn. Ifølge Kunnskapsløftet 2020 er skolen en viktig arena for å gi barn digital kompetanse.[72] Det fremgår i tillegg av rammeverk for grunnleggende ferdigheter at digital kompetanse skal inkludere elementer som nettvett, personvern, informasjonssikkerhet, digital dømmekraft og etisk refleksjon.[73]

72 Utdanningsdirektoratet. (2020, 5. juni). *Utvikle digital kompetanse i skolen.*

Boks 8.9 Dubestemmer.no

Utdanningsdirektoratet har sammen med Datatilsynet utviklet nettressursen Dubestemmer.no. Målet med undervisningsopplegget er å gi økt bevissthet, refleksjon og kunnskap om personvern, og om de valgene barn og unge i alderen 9 til 18 gjør gjennom bruk av digitale medier. Dubestemmer er en populær undervisningsressurs ved mange skoler.[1]

1 Dubestemmer.no

Digital dømmekraft er en samlebetegnelse på juridiske, etiske og moralske forhold som knyttes til bruk av digitale verktøy, ressurser og medier. I rammeverk for grunnleggende ferdigheter forklares det å utøve digital dømmekraft, som å «følge regler for personvern og vise hensyn til andre på nett». Det handler om å «bruke strategier for å unngå uønskede hendelser og å vise evne til etisk refleksjon og vurdering av egen rolle på nett og i sosiale medier.»[74]

Digital dømmekraft inngår også i rammeplanen for barnehagene.[75] Rammeplanen fremhever at barnehagen skal bidra til at barna utvikler en begynnende etisk forståelse knyttet til digitale medier. Det fremgår i tillegg av rammeplanen at personalet skal «utøve digital dømmekraft når det gjelder informasjonssøk, ha et bevisst forhold til opphavsrett og kildekritikk og ivareta barnas personvern».[76] Utdanningsdirektoratet har gratis kompetansepakker som ansatte i skole og barnehage kan benytte seg av.[77]

Når det gjelder lærere, er en del av grunnutdanningen at de skal kunne vurdere og bruke digitale verktøy og ressurser i opplæringen, og kunne gi elevene opplæring i digitale ferdigheter. Lærere skal ha «profesjonsfaglig digital kompetanse» og bruk av digitale verktøy skal være en del av alle fag.[78]

73 Utdanningsdirektoratet. (2017). *Rammeverk for grunnleggende ferdigheter.*

74 Utdanningsdirektoratet. (2017). *Rammeverk for grunnleggende ferdigheter.*

75 Utdanningsdirektoratet. (2017). *Rammeplan for barnehagen.*

76 Utdanningsdirektoratet. (2017). *Rammeplan for barnehagen*, s. 45.

77 Utdanningsdirektoratet. (2022). *Utdanningsdirektoratets kompetanseportal*.

78 Universitetet i Agder, Grunnskolelærerutdanning for trinn 1-7, 5-årig masterprogram.

Det gis altså opplæring i både barnehage og grunnskolen om personvern i instrumentell forstand, for eksempel gjennom digital dømmekraft og nettvett. Selv om dette er viktig for livsmestring i en digital hverdag, mener *kommisjonen* at slik mestring bør understøttes av forståelse av personvern i vid forstand. Så vidt *Personvernkommisjonen* har oversikt over, undervises det i liten grad om personvern som en grunnleggende menneskerettighet, eller i forbindelse med samfunnsfag. En grunnleggende forståelse av hvorfor personvern er viktig for ytringsfrihet og et velfungerende demokrati, er en viktig forutsetning for et opplyst samfunnsliv, og gir nødvendig kontekst for betydningen av digital dømmekraft.

Medieskadelighetsutvalget[79] som overleverte sin rapport i 2021, ser også behovet for å bevisstgjøre barn om personvern. De skriver i sin utredning at mer kunnskap hos barn, unge, foreldre og lærere om den storstilte innsamlingen av personopplysninger som foregår når vi bruker digitale medier, er avgjørende for å kunne håndtere en digital verden.

I Christian Falchs undersøkelse om elevers holdninger til og kunnskap om personvern, kommer det frem at elevene har lav bevissthet om begrepet personvern.[80] Kun tre av elevene kunne forklare hva personvern er. Undersøkelsen avdekker at ingen av deltakerne har hatt undervisning om personvern som tar utgangspunkt i innsamling av personopplysninger og digitale økosystemer. Kunnskapen om grunnleggende digitale ferdigheter og nettvett er imidlertid relativt god. Barna har god bevissthet rundt grunnleggende nettsikkerhet og personvernrelaterte emner som beskyttelse av passord, kildekritikk, mobbing på nett og uønsket bildedeling. Foreldre oppgis som den første og viktigste kilden til kunnskap om grunnleggende nettsikkerhet. Nettvettundervisning på skolen oppgis som neste viktige kilde til kunnskap.

I Falchs samtaler med elevene fremkommer det at elevene har lav bevissthet om hvordan innsamlet informasjon kan påvirke oss. Ingen kjenner egentlig til begrepet persontilpasset innhold. Dette skyldes ikke at barn og unge er kunnskapsløse eller ikke bryr seg. Svarene til elevene reflekterer lav kunnskap om dette i samfunnet generelt og at det ikke undervises i dette i skolen. Ingen av deltakerne i undersøkelsen kan huske at de i skolesammenheng har fått forklart hvordan digitale økosystemer rundt innsamling av personopplysninger fungerer – hverken kommersielt eller samfunnsmessig. Selv om begrepsforståelsen av personvern og bevisstheten om mekanismene for datainnsamling er relativt lav, påpeker Falch at elevene har en praktisk «hverdagsforståelse» av at «noen» samler informasjon om dem. Alle vet at de gir fra seg personlig informasjon i bytte mot gratis apper og tjenester. Det er allmenn aksept for denne «byttehandelen». Alle har sett sammenhengen mellom ting de har vist interesse for på nettet og reklame de har fått etterpå.

> «Alle vet at TikTok overvåker deg på en måte, hvis du har kjøpt deg noe, så blir FYPen din full av akkurat det du har kjøpt», Gutt 12 år, Øvre Vang[81]

Boks 8.10 Nettvett 2.0

Falch trekker frem i sin rapport at det må et fokusskifte inn i skolen i måten man underviser i nettvett og personvern. Dropp pekefingeren. Snakk om muligheter istedenfor problemer. Samtalene med barna har gitt noen gode innspill til «Nettvett versjon 2.0».

- Synliggjør «usynlige» strukturer som digitale økosystemer – har man kartet er det lettere å navigere selv.
- Bruke andre ord når man snakker om digitale problemstillinger. Ved å snakke om muligheter og verdier fremfor farer og forbud, oppnår man å skape mer nysgjerrighet, engasjement og forståelse.
- Fokuser på mulighetene i digitale verktøy fremfor de problemene de skaper.
- Fokuser på verdier. Våre egne personopplysninger er et godt eksempel på en verdi vi bør ta vare på og være bevisst.
- Fokuser på mennesker. Hvem lager de digitale løsningene? Alle digitale løsninger er lagd av mennesker som deg og meg. Det er ikke bare programvareutviklere, men også for eksempel atferdspsykologer eller forskjellig typer designere. Hvordan tenker de? Hvordan tenker de som lager Google?[1]

[1] Falch, C. (2022). *Rapport til Personvernkommisjonen. Intervjuer med barn og unge om personvern.*

[79] NOU 2021: 3 *Barneliv foran, bak og i skjermen. Utvalg for beskyttelse av barn og unge mot skadelig medieinnhold – med særlig vekt på pornografisk og seksualisert innhold.*

[80] Falch, C. (2022). *Rapport til Personvernkommisjonen. Intervjuer med barn og unge om personvern.*

Et interessant funn i Falchs undersøkelse er at barna trekker frem at måten å snakke om digitale problemstillinger på er avgjørende for engasjement og forståelse. Elevene er lei av problemfokuset og ønsker heller å lære om muligheter og verdier. Basert på samtalene med elevene, konkluderer Falch i sin rapport med at tiden er inne for å bevege seg vekk fra den problemorienterte nettvettundervisningen til en mer kunnskapsorientert undervisning som fokuserer på hvordan digitale verktøy virker og påvirker den enkelte og samfunnet som helhet.

> «Åhh, jeg er lei nettvettgreier, man snakker bare om alt man ikke skal gjøre», Gutt 11 år, Innlandet[82]

Personvernkommisjonen mener skolen må styrke opplæringen på personvern som en grunnleggende menneskerettighet. Elever bør få opplæring i de samfunnsfaglige sidene ved personvern, herunder at godt personvern er en viktig verdi i et demokratisk samfunn. Undervisning om personvern i skolen kan bidra til at elevene får et mer bevisst forhold til at deres personopplysninger behandles, og innsikt i hva digitale læringsverktøy samler inn av opplysninger. *Kommisjonen* understreker at ansvaret for å ivareta eget personvern ikke skal legges på den enkelte elev. Opplæring av barn er viktig for å gi dem tilstrekkelig ballast, men skal ikke ses som løsning på personvernutfordringene i skolen, snarere noe som kommer på toppen av de tiltak som *kommisjonen* anbefaler.

8.4.8 Barn og foresattes rettigheter

For barn og unge i skolen og barnehagen, handler personvern om at foresatte og barn skal vite om og ha kontroll over hvordan opplysningene om barna blir brukt. Informasjon til foresatte og barna om hvorfor og hvordan opplysningene om barna blir behandlet, er en grunnleggende personvernrettighet. Uten informasjon har foresatte og barn ingen mulighet til å si ifra hvis de mener skolen og barnehagen ivaretar personvernet på en dårlig måte. Uten informasjon har de heller ikke mulighet til å bruke sine andre rettigheter etter personvernforordningen, slik som retten til å be om innsyn, retting eller sletting eller å protestere på behandlingen.

8.4.8.1 Åpenhet og informasjon

Digitaliseringen av skolen fører til at skolene og kommunen etter hvert vil sitte på stadig større datamengder om elevene. For at skolene skal ivareta tillitsforholdet de har til elevene og deres foresatte, er det derfor ekstra viktig at skolene fremover gir tydelig og god informasjon om hvilke data verktøyene samler inn og hvordan de brukes.

Personvernkommisjonen har i innspillsseminar med Elevorganisasjonen og Foreldreutvalget for grunnopplæringen (FUG) fått tilbakemelding om at skoler og skoleeiere ikke gir tilstrekkelig informasjon om hvilke personopplysninger de digitale verktøyene samler inn og til hvilke formål opplysningene benyttes. Kommunene har videre ikke gode nok rutiner for å gi informasjon om, og håndtere, retten til innsyn. Kommunene må ha systemer og rutiner på plass for å kunne besvare en anmodning om informasjon og innsyn, uavhengig av om informasjon er lagret i kommunens systemer, på den enkelte skole, eller hos en databehandler.

Den overnevnte undersøkelsen til Christian Falch bygger opp under tilbakemeldingen fra Ele-

Boks 8.11 Forslag fra barna til hvordan skolen kan gi informasjon

I Christian Falchs rapport kommer barna med mange gode forslag til hvordan skolen kan gi bedre informasjon til barna og foreldrene om personvernspørsmål. Barna er opptatt at av skolen må gi informasjon som barn og foreldre kan se på og forstå i fellesskap. Det må ikke være et skriv som foreldrene får på et foreldremøte og så kaster når de kommer hjem. Det er også viktig at informasjon gis til riktig tid. Informasjonen bør knyttes direkte opp mot konkrete hendelser, for eksempel når man får læringsbrett, eller før man skal på ungdomsskolen og begynner med karakterer. Barna i undersøkelsen til Christian Falch foreslår at læringsbrettet kan brukes til å vise hvordan apper og tjenester deler personopplysninger. På den måten får elevene er mer «hands on»-følelse med hva de forskjellige appene og tjenestene faktisk deler av personopplysninger om elevene.[1]

[1] Falch, C. (2022). Rapport til *Personvernkommisjonen. Intervjuer med barn og unge om personvern*.

[81] Falch, C. (2022). *Rapport til Personvernkommisjonen. Intervjuer med barn og unge om personvern*.

[82] Falch, C. (2022). *Rapport til Personvernkommisjonen. Intervjuer med barn og unge om personvern*.

vorganisasjonen og FUG. Ingen av elevene intervjuet i undersøkelsen til Falch kan huske å ha fått informasjon om hva skolen samler inn av personopplysninger om dem. Ingen har heller fått informasjon om hva digitale verktøy som læringsbrett og PC-er med tilhørende programvare, samler av personopplysninger om dem.

Personvernkommisjonen mener kommunene må sørge for at informasjon om hvilke opplysninger som samles inn om elevene og barnehagebarna er lett tilgjengelig.

Mangel på åpenhet og kontroll over hvilke opplysninger som samles inn og hvordan de brukes, kan føre til mistillit mellom skole og elev/ hjem. Når skolen er åpen om formålet kan elevene ha et aktivt og kritisk forhold til bruken av de digitale læringsverktøyene.

Personvernkommisjonen vil imidlertid påpeke at informasjon ikke er en løsning, men en forutsetning for godt personvern, og noe som kommer i tillegg til de andre tiltak som *kommisjonen* anbefaler.

8.4.8.2 Rett til å protestere

Når behandling av personopplysninger skjer med grunnlag i «allmennhetens interesse eller for å utøve offentlig myndighet»,[83] har elever som det er registrert opplysninger om rett til å protestere på behandlingen.[84] Protester må være begrunnet i elevens «særlige situasjon».[85] Skoleeier har plikt til å legge til rette for at elever/foreldre kan bruke denne rettigheten. De må derfor sørge for at skolen har rutiner som gjør denne rettigheten synlig og grei å bruke.

Retten til å protestere er særlig viktig fordi skoler og barnehager trolig i økende grad vil ta i bruk persontilpasset undervisning og læringsanalyse. Slike metoder innebærer mer utstrakt bruk av personopplysninger om barna. Maktforholdet mellom skoleeier på den ene side og elever og foresatte på den andre, er skjevt. Retten til å protestere gir den enkelte et middel til å motsette seg at skolen bruker opplysninger elevene ikke ønsker skal bli brukt. Elevenes/ foresattes mulighet til å protestere gir også en grunn for skoleeier til å velge systemløsninger og rutiner som gjør at retten til å protestere sjelden blir aktuell å bruke.

Protest mot å behandle opplysninger kan være problematisk hvis skolen dermed ikke kan behandle personopplysninger som er nødvendige for å gi elevene et fullgodt tilbud. For eksempel kan protesten gjelde opplysninger som er viktig for evalueringen av eleven eller for tilbud om individuelt tilpasset undervisning. Skoleeier plikter imidlertid å motvirke at det blir negative konsekvenser av å bruke retten til å protestere, for eksempel ved å ha et så godt alternativt opplegg som mulig for den som har protestert. Negative konsekvenser som er uunngåelige, må elevene ta hensyn til når de vurderer om de vil bruke retten til å protestere eller ikke. Uansett kan det tenkes situasjoner der en protest vil skape så store, uunngåelige negative konsekvenser at det gir skoleeier «tvingende berettigede grunner» til å bestemme at elevenes rettigheter må vike. Selv om det skal mye til for at retten til å protestere kan bli satt til side på en slik måte, kan dette forekomme.

Dersom mange elever ved en skole bruker retten til å protestere, kan skoleeier komme i en vanskelig situasjon. Antallet protester vil imidlertid kunne begrenses ved å ikke behandle andre opplysninger enn nødvendig for behandlingsformålet og generelt sørge for forsvarlig behandling av data.

Personvernkommisjonen anser det som avgjørende at verktøy ikke blir introdusert uten at det er vel begrunnet, og i samsvar med personvernregelverket.

8.4.8.3 Medvirkning

God informasjon er en forutsetning for at foreldre og elever skal ha mulighet til å medvirke eller påvirke hvilke digitale læringsmidler og systemer som benyttes i skolen. *Personvernkommisjonen* har fått innspill i innspillsseminar om at manglende kunnskap og informasjon fra skole og skoleeier gjør at foresatte i praksis ikke har mulighet til å engasjere seg eller medvirke i beslutninger.

Kartlegging og måling av barns ferdigheter vil bare øke i årene som kommer. Datatilsynet har vært kritiske til en utvikling der kartleggingsverktøy i stadig større grad blir brukt overfor barn uten at foreldrene samtykker til dette.[86] *Personvernkommisjonen* er skeptisk til om samtykke er løsningen, da dette kan stille elever ulikt, avhengig av hva foreldrene samtykker til, og det kan i praksis blir vanskelig for skole/skoleeier å administrere. *Kommisjonen* anser det i stedet som avgjørende at foreldrene har mulighet til å gi innspill og delta aktivt ved utforming og implementering av slike kartleggingsverktøy.

---

[83] Se personvernforordningen artikkel 6 nr. 3

[84] Se personvernforordningen artikkel 21 nr. 6.

[85] Se personvernforordningen artikkel 21 nr. 6.

[86] Datatilsynet. (2014). *Årsmelding for 2014.*

Boks 8.12 AVT-prosjektet og bruk av interessentinvolvering

Gjennom deltakelse i sandkassen ønsker AVT-prosjektet å utforske de rettslige rammene, i tillegg til rammene for ansvarlighet og etikk, for bruk av læringsanalyse i skolen. I workshopen deltok både elever, foresatte, lærere og personvernombud fra kommunene som samarbeider med AVT-prosjektet. Funnene følger nedenfor.

Risiko for endret atferd/nedkjølingseffekt

Elevene var særlig bekymret for å bli overvåket på hvor lang tid de bruker på oppgavene. De påpekte at en slik tidtaking kan oppleves som et press om å løse oppgavene raskest mulig, på bekostning av kvalitet og læringsutbytte av oppgaveløsingen.

Risiko for ukorrekte personopplysninger i systemet

En potensiell kilde til ukorrekte opplysninger, som ble diskutert blant de voksne deltagerne på workshopen, kan oppstå hvis en elev løser oppgaver på andre elevers vegne. En lignende feilkilde kan være at noen elever bevisst svarer feil for å manipulere systemet til å få lettere eller færre oppgaver. Risikoen for dette har nok eksistert i skolen i alle år, og det er ingen grunn til å tro at overgangen til digital oppgaveløsing har endret på det. Konsekvensene for den enkelte elev kan imidlertid bli større dersom data fra oppgaveløsingen inngår i en KI-basert profilering av eleven. For eksempel ved at systemet lures til å tro at eleven er på et høyere nivå enn vedkommende egentlig er, og dermed anbefaler oppgaver som eleven ennå ikke har forutsetninger for å kunne løse.

Risiko for at teknologien påfører elevene uønsket stress

Elevene uttrykte bekymring for at det ville bli en forventning om å vise frem «scoren» sin i systemet til medelever og foreldre, på samme måte som elever i dag kan oppleve et press om å dele prøveresultater. Ved bruk av læringsanalysesystemet risikerer man at skillet mellom øvings-/læringssituasjonen og testing blir mer uklart for elevene. Lærerne bruker også i dag informasjon fra elevenes oppgaveløsning og deltagelse i skoletimene som grunnlag for å vurdere elevenes kunnskapsnivå. Ved bruk av læringsanalysesystemet vil imidlertid denne vurderingen systematiseres og visualiseres på en annen måte enn i dag.[1]

[1] Datatilsynet. (2022). *AVT. Sluttrapport fra sandkasseprosjektet med KS, SLATE ved UiB og Utdanningsetaten i Oslo kommune*.

I innspillseminar med *Personvernkommisjonen* trakk Elevorganisasjonen frem at elevene mangler gode og effektive medvirkningsmuligheter knyttet til ivaretakelse av elevenes personvern. De trakk særlig frem videoovervåkning i skoletiden som en personvernutfordring der de opplever at elevenes perspektiv ikke er hensyntatt i tilstrekkelig grad. Elevorganisasjonen mener videoovervåking i skoletiden utgjør en for stor innskrenkning av personvernet sett opp mot fordelene ved slik overvåkning. Ifølge Elevorganisasjonen stopper ikke videoovervåkning uønskede hendelser, og fører i stedet til at elever tilpasser atferden sin. Organisasjonen etterlyste et totalforbud mot videoovervåkning i skoletiden.

Et annet eksempel på en problemstilling der Elevorganisasjonen mener elevene burde bli involvert, er pålegg om å ha kamera på pcen påslått i forbindelse med digital undervisning. Under covid-19-pandemien uttalte flere i skolesektoren at lærere burde kunne kreve at elevene skrur på kamera under undervisningen, forutsatt at dette var pedagogisk begrunnet.[87] Det kan være mange gode grunner til at lærerne ønsker å se elevene, som for eksempel kontroll av deltakelse og fravær, og for å kunne gi tilbakemelding og veiledning. Elevorganisasjonen pekte i et intervju med Utdanningsnytt på at mange elever føler seg ukomfortable foran kamera av ulike grunner. Organisasjonen viste for eksempel til at enkelte elever skammer seg over hjemmet de bor i eller at det er flere andre familiemedlemmer hjemme som ikke ønsker å bli eksponert foran kamera til hele klassen.[88]

[87] Utdanningsnytt. (2021, 3. januar). *Digital undervisning: – Kan kreve at elevene slår på kameraet.*

I forbindelse med vurderinger av personvernkonsekvenser, skal den behandlingsansvarlige, dersom det er relevant, innhente synspunkter på den planlagte behandlingen fra de registrerte eller deres representanter. *Personvernkommisjonen* anser at å innhente registrertes synspunkter er et viktig risikoreduserende tiltak i forbindelse med innføring av tiltak som innebærer behandlinger av personopplysninger med høy risiko for de registrertes rettigheter og friheter. Også Datatilsynet har gjort funn i prosjektet «Aktivitetsdata for vurdering og tilpassing» (AVT), som deltok i Datatilsynets sandkasse i 2022, som underbygger interessentinvolveringen som et viktig tiltak for å identifisere og redusere personvernrisiko.[89]

Personvernkommisjonen mener kommunene bør legge til rette for reelle medvirkningsmuligheter for elever og foresatte i beslutninger som berører barnas personvern i vesentlig grad. Elever og foresatte kan involveres på ulike måter, blant annet i forbindelse med gjennomføringen av personvernkonsekvensvurderinger. Andre medvirkningsarenaer der skoleeier kan innhente og diskutere synspunkter med elever og foresatte er i Elevutvalget, FAU og Foreldreutvalget for grunnopplæringen (FUG).

8.5 Personvernkommisjonens anbefalinger oppsummert

Nasjonale føringer

– *Personvernkommisjonen* mener det må etableres en helhetlig og offensiv statlig personvernpolitikk i skole- og barnehagesektoren. *Kommisjonen* mener at den nasjonale personvernpolitikken for barnehage og skole må:
  - sette kommuner, skoler og barnehager i stand til å bruke digitale tjenester og læringsverktøy på en måte som ivaretar barns og unges personvern.
  - sørge for at både barns rett til utdanning og rett til vern av personopplysninger ivaretas, samtidig som kommunalt selvstyre og metodefrihet i skolen og barnehagen bevares.
  - stille tydelige krav til kvaliteten på de digitale tjenestene også hva angår personvern.
  - inneholde og konkretisere krav til at leverandører av tjenester til skole- og barnehagesektoren ikke kan benytte forretningsmodeller som profitterer kommersielt på barn personopplysninger. I praksis betyr dette at det ikke er akseptabelt å benytte leverandører som forbeholder seg retten til å bruke barn og unges data til kommersielle formål, spesielt markedsføringsaktiviteter.
  - fange opp tiltak som kommer frem i arbeidet til Ekspertutvalget som er nedsatt for å se på personvernutfordringer knyttet til bruk av læringsanalyse.
– *Personvernkommisjonen* mener behovet for en nasjonal tjenestekatalog er stort, og kan være et viktig initiativ for i praksis å sørge for at skoleeiere kan velge tjenester som ikke bare er funksjonelle, men også ivaretar personvern på en tilfredsstillende måte. Det må sikres at tjenestekatalogen stiller klare og etterprøvbare krav til personvern og informasjonssikkerhet. Tjenestekatalogen bør gi oversikt over læremidler der det er gjennomført risiko- og sårbarhetsanalyse og personvernkonsekvensvurderinger. En velfungerende tjenestekatalog forutsetter kontinuerlige endringer og oppdateringer, da digitale tjenester kan endres fortløpende.
– *Personvernkommisjonen* mener statlige myndigheter må ta initiativ til å utarbeide en personvernnorm for skole- og barnehagesektoren. En personvernnorm kan bidra til å sette kommunene bedre i stand til å ivareta behandlingsansvaret sitt og sikre en mer helhetlig og omforent ivaretakelse av barns personvern i barnehagen og grunnskolen. En norm kan også bidra til å forenkle kommunenes anskaffelsesprosesser ved å oppstille krav som leverandørene må etterleve og vil være kjent med.

Kompetanse og ressurser

– *Personvernkommisjonen* mener det er avgjørende for personvernet til barn i skole og barnehage at kommunene sikres tilstrekkelige personvernressurser, herunder tilgang på ressurser med grunnleggende teknologikompetanse. Dette er en forutsetning for å kunne gjøre gode vurderinger og ivareta personvernet på løpende basis.
– *Personvernkommisjonen* anbefaler derfor at det etableres, eller videreutvikles i allerede eksisterende strukturer, et tverrfaglig nasjonalt test-

[88] Utdanningsnytt. (2021, 3. januar). *Digital undervisning: – Kan kreve at elevene slår på kameraet.*

[89] Datatilsynet. (2022). *ATV. Sluttrapport fra sandkasseprosjektet med KS, SLATE ved UiB og Utdanningsetaten i Oslo kommune.*

og kompetansemiljø som ivaretar følgende funksjoner:

- *Kompetansemiljø som koordinerer og utvikler verktøy og malverk* som setter kommunene i stand til å gjennomføre risikovurderinger og personvernkonsekvensvurderinger og å etablere effektiv internkontroll.
- *Testing* av digitale løsninger som skal brukes i skoler og barnehager. Resultatene fra testingen av løsningene bør kommuniseres videre til de ansvarlige for den nasjonale tjenestekatalogen.
- *Forhandlingsledelse og forhandlingsstøtte* til kommunene i forhandlinger med plattformleverandørene. Dette vil styrke kommunenes forhandlingsmakt ved at det vil være lettere å stille nødvendige krav til tjenestene.

Rutiner og veiledning

– *Personvernkommisjonen* mener kommunene i større grad må sørge for tilpassede rutiner og veiledning til skoleledelse og lærere. Det bør blant annet utarbeides retningslinjer som klargjør roller og ansvar knyttet til anskaffelse og bruk av nye digitale læringsverktøy.
– *Personvernkommisjonen* mener Utdanningsdirektoratet i større grad bør hjelpe og tilrettelegge for at kommunene kan ivareta sitt behandlingsansvar etter personvernregelverket. Dette innebærer blant annet at kommunene får bistand til å etablere nødvendige og tilpassede rutiner og veiledning.
– *Personvernkommisjonen* mener det er viktig at kommunene har rutiner som sikrer at barns personvern ivaretas når digitale verktøy benyttes utenfor skolens område. Dette betyr blant annet å tydeliggjøre eventuelle begrensninger i skolens ansvar, og å utarbeide retningslinjer for hvordan foreldre kan bidra til å ivareta sine barns personvern ved bruk av digitale verktøy utenfor skolen. Endelig bør kommunene regelmessig følge opp og vurdere om tiltakene og rutinene til enhver tid er tilstrekkelige.
– *Personvernkommisjonen* mener det er viktig at kommunene har rutiner og retningslinjer som sikrer at lærere og andre ansatte ved skolen ikke bruker opplysninger som samles inn og lagres i elevenes digitale enheter til kontrollformål. Kommunen må også lage rutiner som påser at elever og foreldre informeres om hvilke opplysninger som samles inn og hva de brukes til.
– *Personvernkommisjonen* mener det vil være synergieffekter å hente ut for kommunene hvis de samarbeider med andre kommuner om utarbeidelse av veiledende rutiner.
– Som ledd i arbeidet med å styrke internkontrollen i skole- og barnehagesektoren, mener *Personvernkommisjonen* at lærere og barnehagelærere må få bedre opplæring i personvern og hensynene bak personvernregelverket.

Bruk av elevers personopplysninger til kommersielle formål

– *Personvernkommisjonen* mener regjeringen må ta initiativ til en bred utredning om digitale verktøy som er i bruk i skolen og hvordan de påvirker barns personvern. En slik utredning bør gjelde alle typer læremidler og øvrige metoder og verktøy som brukes i undervisningssammenheng. Hvilke overvåkningsmuligheter disse verktøyene gir, hvilken kunnskap det er mulig å trekke ut av opplysningene som samles inn og lagres og hvordan kunnskapen blir brukt til nytte for elever og for utdanningsinstitusjoner, bør belyses i en slik utredning. Videre bør det kartlegges hvordan personopplysningene som samles inn viderebehandles til ulike formål. *Kommisjonen* anser at det er sentralt å vurdere dette også fra et datastrategisk perspektiv. Data om norske elevers læringsmønstre er strategisk viktige, og kan ikke overlates til kommersielle aktører for videre bruk, eller på måter der Norge reelt sett gjør seg avhengig av disse aktørene.
– *Personvernkommisjonen* mener annonseblokkeringsverktøy eller andre tiltak på elevenes utstyr må vurderes som et tiltak for å redusere elevenes eksponering mot reklame. Dette kan i tillegg bidra til å redusere sporingen av elevenes digitale aktivitet til kommersielle formål.

Innkjøp og forhandlinger

– *Personvernkommisjonen* mener innkjøp og forhandlinger, spesielt fra de store plattformleverandørene, bør profesjonaliseres og sentraliseres. Statlige myndigheter og/eller KS bør gå aktivt inn å bistå kommunene i forhandlinger med plattformleverandørene for å avhjelpe maktskjevheten mange småkommuner står i. Ved å styrke forhandlingsmakten vil det være lettere å stille nødvendige krav til tjenestene som skal behandle personopplysninger om elever og barnehagebarn.

- *Personvernkommisjonen* mener statlige myndigheter bør se på muligheten for å inngå samarbeid med andre land i forhandlinger med de globale plattformleverandørene, for eksempel innenfor rammen av det nordiske samarbeidet.
- *Personvernkommisjonen* mener innkjøp og forhandlinger om løsninger til skole- og barnehagesektoren må forankres i den nasjonale personvernpolitikken for skolen og barnehagen. Denne politikken må inneholde tydelige krav til kvaliteten på læringsmidlene, samtidig som de ivaretar barns rett til personvern og vern mot at data som samles inn om elevene benyttes til kommersielle formål.

Utvikling av forsvarlige digitale læringsmidler

- *Personvernkommisjonen* mener den nasjonale personvernpolitikken for skole- og barnehagesektoren bør inneholde tiltak for å støtte norske virksomheter som utvikler løsninger som bygger opp under prinsippene i den nasjonale utdanningspolitikken og barns grunnleggende rettigheter – og som ikke bygger på en forretningsmodell som profiterer på barns personopplysninger.
- *Personvernkommisjonen* mener at dersom vurderinger gjennomført av det nasjonale test- og kompetansesenteret viser at eksisterende løsninger ikke ivaretar personvernet på en tilfredsstillende måte, må statlige myndigheter investere i utvikling av nye, forsvarlige løsninger. *Kommisjonen* anser at det kan være hensiktsmessig å gjøre slike investeringer i europeisk eller nordisk regi. Norge kan, og bør etter *kommisjonens* syn, ta en foregangsrolle i dette arbeidet.

Undervisning i personvern

- *Personvernkommisjonen* mener skolen må styrke opplæringen på personvern som en grunnleggende menneskerettighet. Elever bør få opplæring i de samfunnsfaglige sidene ved personvern, herunder at godt personvern er en viktig verdi i et demokratisk samfunn. Undervisning om personvern i skolen kan bidra til at elevene får et mer bevisst forhold til at deres personopplysninger behandles, og innsikt i hva digitale læringsverktøy samler inn av opplysninger. *Kommisjonen* understreker at ansvaret for å ivareta eget personvern ikke skal legges på den enkelte elev. Opplæring av barn er viktig for å gi barna tilstrekkelig ballast, men skal ikke ses som løsning på personvernutfordringene i skolen, snarere noe som kommer på toppen av de tiltak som *kommisjonen* anbefaler.

Ivaretakelse av barnas og foresattes rettigheter

- *Personvernkommisjone*n mener kommunene må sørge for at informasjon om hvilke opplysninger som samles inn om elevene og barnehagebarna er lett tilgjengelig.
- *Personvernkommisjonen* mener kommunene bør legge til rette for reelle medvirkningsmuligheter for elever og foresatte i beslutninger som berører barnas personvern i vesentlig grad. Elever og foresatt kan involveres på ulike måter, blant annet i forbindelse med gjennomføringen av personvernkonsekvensvurderinger. Andre medvirkningsarenaer der skoleeier kan innhente og diskutere synspunkter med elever og foresatt er i Elevutvalget, FAU og Foreldreutvalget for grunnopplæringen (FUP).

Kapittel 9
Forbrukernes personvern

9.1 Innledning

Personvernkommisjonen skal ifølge mandatet kartlegge «forbrukeres reelle muligheter til å ivareta eget personvern ved bruk av digitale løsninger og tjenester». Herunder skal *kommisjonen* vurdere om «bransjenormer, merkeordninger eller sertifiseringsmekanismer kan brukes bedre». *Personvernkommisjonen* skal videre «utrede hvilke konsekvenser bruk av sosiale medier har for innsamling, analyse og viderebruk av personopplysninger». *Kommisjonen* skal på bakgrunn av dette foreslå tiltak for å «sikre personvernet, herunder den enkelte borgers mulighet for å ivareta eget personvern».

Kommisjonen oppfatter problemstillingene knyttet til forbrukeres personvern ved bruk av digitale tjenester og personvernet til brukere av sosiale medier, som overlappende. De to mandatpunktene vil derfor bli behandlet samlet. Der problemstillinger knytter seg særlig til sosiale medier, vil *Personvernkommisjonen* fremheve dette. *Kommisjonen* tolker begrepet «forbruker» i vid forstand, da digitale forbrukertjenester og plattformer som for eksempel sosiale medier brukes til en rekke formål og i mange forskjellige sammenhenger som gjør det utfordrende og tidvis uhensiktsmessig å trekke klare skiller mellom blant annet forbruker- og innbyggerrollen.

For å beskrive hvordan personvernet til forbrukerne påvirkes i dag, vil *Personvernkommisjonen* i dette kapitlet peke på hva som kjennetegner en forbruker av digitale tjenester og hvorfor forbrukere er sårbare i dag, samt hvordan sårbarheten arter seg. *Kommisjonen* ønsker også å si noe om hvilke faktorer som bidrar til at personvernet til forbrukerne er under press, herunder hvorfor personopplysninger samles inn, hva de brukes til og hvordan virksomheter tjener penger på personopplysninger.

I dag foregår en stadig større del av forbrukernes hverdag digitalt. Smarttelefoner og tilkoblede produkter har ført til at mennesket er digitalt tilkoblet tilnærmet døgnet rundt. Flere av verdens største selskaper er globale teknologiselskaper som har innsamling og bruk av personopplysninger som kjernevirksomhet, slik som Alphabet (Google), Meta (Facebook) og Amazon. Personopplysninger brukes til å utvikle og tilpasse tjenester basert på enkeltpersoners eller gruppers behov. Samtidig brukes personopplysninger til å målrette markedsføring. Innsamling og bruk av personopplysninger er ikke i seg selv problematisk, og kan være en forutsetning for utvikling av mange gode forbrukertjenester. Det er likevel en forutsetning for ivaretakelse av forbrukernes personvern at innsamling og bruk av personopplysninger skjer på en åpen, rettferdig og forståelig måte, og ikke er mer omfattende enn nødvendig.

Det er i dag krevende for forbrukerne å ha oversikt og kontroll over hvordan opplysninger om dem samles inn og brukes. Undersøkelser viser at mangelen på oversikt og kontroll har ført til at mange forbrukere oppgir at de føler en form for resignasjon når det kommer til ivaretakelse av personvernet sitt. Undersøkelser viser også at forbrukernes opplevelse av mangel på kontroll, fører til tap av tillit til enkelte digitale tjenesteleverandører, særlig til de globale plattformselskapene.[1]

Ettersom en stor andel av de mest populære digitale forbrukertjenestene drives av internasjonale selskaper, har Norge et begrenset nasjonalt handlingsrom. Mange av de viktigste prosessene knyttet til regulering og håndheving skjer på europeisk nivå. Det betyr ikke at Norge er maktesløse. Som *Personvernkommisjonen* vil peke på i dette kapitlet, kan norske myndigheter ta tydelige standpunkter som kan ha internasjonal effekt. Arbeidet med å sikre norske forbrukeres personvern bør skje gjennom aktivt samarbeid med EU og andre lands myndigheter.

9.1.1 Begreper og definisjoner

En *forbruker* defineres vanligvis som en fysisk person som kjøper en vare eller en tjeneste utenfor

[1] Datatilsynet. (2020). *Personvernundersøkelsen 2019/20.*

næringsvirksomhet eller yrke, der tingen eller tjenesten hovedsakelig er til privat bruk. Denne definisjonen skiller såkalte forbrukerkjøp fra transaksjoner som skjer i næring, for eksempel mellom næringsvirksomheter og andre, juridiske personer eller institusjoner.[2]

Forbrukerne skal ha god og tilstrekkelig informasjon om varer og tjenester som tilbys i markedet, og kunnskap om sine rettigheter som forbruker. Informasjon fremmer forbrukermakt og gjør det mulig for forbrukerne å ta opplyste valg. Den digitale forbrukerrollen karakteriseres også av at forbrukere går fra å være kunder til å være brukere av mange tjenester. For eksempel er det ikke alltid mulig å skille når forbrukerrollen slutter og innbyggerrollen begynner når man deltar i en politisk diskusjon eller oppsøker informasjon fra myndighetene i sosiale medier. Flere av problemstillingene som drøftes i dette kapitlet vil derfor gjelde forbrukerrollen i utvidet forstand, og kan overlappe med andre samfunnsroller den enkelte har.

Digitale forbrukertjenester omfatter blant annet sosiale medier, søkemotorer, markedsplasser, digitale plattformer og e-handelstjenester.[3] Eksempler på digitale tjenester er ulike fitness- og helseapper, nettbutikker, plattformtjenester som AirBnB, samt diverse verktøy som Google Søk. I tillegg er stadig flere forbrukerprodukter utstyrt med programvare, sensorer og andre digitale komponenter. Slike produkter kan samles under betegnelsen *tingenes internett*.

I den digitale forbrukerhverdagen er mange populære tjenester tilgjengelig for gratis bruk, for eksempel fordi tjenestene er reklamefinansierte eller fordi tjenestetilbyderne tjener penger på bruk eller salg av personopplysninger samlet inn fra brukerne. Selv om brukerne av såkalte gratis tjenester ikke nødvendigvis vil oppfatte bruken av tjenesten som en del av et kundeforhold, fordi det ikke involverer en pengetransaksjon, vil bruken fortsatt omfattes av forbrukerbegrepet, og følgelig behandles i dette kapitlet.

Begrepet *plattformer* omfatter blant annet online markedsplasser, sosiale medier, appbutikker, prissammenligningstjenester, delingsøkonomitjenester og søkemotorer. Fellestrekk for plattformer inkluderer bruk av kommunikasjons- og informasjonsteknologi for å muliggjøre interaksjon mellom brukere, innsamling og bruk av data om interaksjoner, samt nettverkseffekter der antallet brukere øker nytteverdien av plattformen.[4]

Atferdsbasert markedsføring er ikke et eksakt definert begrep. I praksis brukes begrepet om reklame basert på observasjon av atferden til individer over tid. Atferdsbasert markedsføring er basert på utledning av egenskaper fra analyse av handlinger (gjentatte nettstedsbesøk, interaksjoner, søkeord, tid brukt på innhold, osv.) for å utvikle en bestemt profil og skreddersy annonser til enkeltpersoner for å matche deres antatte interesser. Atferdsbasert markedsføring omtales tidvis også som tilpasset eller målrettet markedsføring.[5] Målretting kan være basert på atferd som beskrevet over. Målretting kan imidlertid også være basert på annen informasjon, som data som en person oppgir direkte, for eksempel adresse eller kjønn. I det følgende bruker *Personvernkommisjonen* begrepet atferdsbasert markedsføring for enkelhets skyld.

9.1.2 Politiske føringer for ivaretagelse av forbrukernes personvern

Norske myndigheter har i løpet av de siste årene publisert en rekke stortingsmeldinger og strategier om digitaliseringen av forbrukerhverdagen. Selv om disse som regel omhandler de positive endringene digitaliseringen bidrar til, er personvernutfordringer et gjennomgående tema.

I Meld. St. 25 (2018–2019) *Framtidas forbrukar – grøn, smart og digital*, peker Solberg-regjeringen på at målsetningen om datadreven innovasjon skaper betydelige personvernutfordringer for forbrukerne, blant annet på grunn av mangel på kontroll og informasjon til forbrukerne. Det påpekes at Solberg-regjeringen ønsker en utvikling hvor forbrukere i større grad kan velge personvernvennlige alternativer, og at personvern blir et konkurransefortrinn.[6] Dette skal blant annet skje gjennom styrket kunnskap om personvern blant forbrukere og næringslivsaktører og gjennom internasjonalt samarbeid for å styrke personvernet. Personvern er også en del av et større bilde, og det fremgår at Solberg-regjeringen vil «leggje vekt på betre tilsyn med reglane og styrkt samarbeid mellom styresmaktene i politikk som gjeld forbru-

2 Se lov 21. juni 2002 nr. 34 om forbrukerkjøp (forbrukerkjøpsloven) § 2 og lov 17. juni 2022 nr. 56 om levering av digitale ytelser til forbrukere (digitalytelsesloven) § 1

3 Hva som omfattes av begrepet digitale forbrukertjenester er for eksempel definert i forslag til Forordning om digitale tjenester (Digital Services Act – DSA)

4 Europakommisjonen. (2022, 7. juni). *Online platforms.*

5 Article 29 Data Protection Working Party. (2010). *Opinion 2/2010 on online behavioural advertising.*

6 Meld. St. 25 (2018–2019) *Framtidas forbrukar – grøn, smart og digital.* Barne- og familiedepartementet.

karsaker, personvern, IKT-tryggleik og konkurranse.»[7]

Meld. St. 22 (2020–2021) *Data som ressurs – Datadrevet økonomi og innovasjon* omhandler hvordan dataøkonomien kan bli en sterk driver for økonomisk vekst. Det inkluderer blant annet ambisjoner om økt datadeling mellom offentlig og privat sektor, samt å tilrettelegge for at Norge kan spille en aktiv part i dataøkonomien. I meldingen understrekes det at dette ikke skal skje på bekostning av personvernet, og at personvern er nødvendig for å bevare tillit i samfunnet. Kommersialisering av personopplysninger, manglende informasjon og kontroll, samt manglende håndheving av grensekryssende saker trekkes fram som noen hovedutfordringer for forbrukernes personvern. Det fremgår også her at personvern bør være et konkurransefortrinn.

> «Ansvarlig og etisk bruk av data er viktig for å bevare tilliten i det norske samfunnet. Deling og bruk av data skal skje på en måte som ivaretar individets rettigheter og friheter. For eksempel kan økt deling og bruk av personopplysninger til nye formål utfordre personvernet og den enkeltes autonomi. Virksomheter som deler og bruker data, skal ikke bare vurdere lovligheten i bruken av personopplysninger og andre sensitive data, men også foreta en etisk vurdering.»
>
> Meld. St. 22 (2020–2021)
> *Data som ressurs – Datadrevet økonomi og innovasjon*[8]

I 2021 lanserte Solberg-regjeringen *Rett på nett – Nasjonal strategi for trygg digital oppvekst*. Denne strategien omhandler barn og unges digitale hverdag.[9] Det pekes på at det kreves et kunnskapsløft om personvern blant barn og unge, at tilsyn med digital markedsføring mot barn må koordineres og styrkes, og at plattformer må ansvarliggjøres, blant annet gjennom den kommende forordningen om digitale tjenester (Digital Services Act, DSA).

I 2020 lanserte Solberg-regjeringen sin «Nasjonale strategi for kunstig intelligens». Strategien peker på personvern som et sentralt prinsipp for ansvarlig og etisk bruk og utvikling av kunstig intelligens:

> «Regjeringen vil at Norge skal gå foran i utvikling og bruk av kunstig intelligens med respekt for den enkeltes rettigheter og friheter. Kunstig intelligens i Norge skal bygge på etiske prinsipper, respekt for personvernet og god digital sikkerhet.»[10]

Videre sier strategien at «Norske myndigheter har fulgt EUs arbeid med modernisering av forbrukerrettighetene tett, og vil også gjøre dette fremover.»[11]

Personvernkommisjonen mener Regjeringen bør være en aktiv pådriver i EUs lovgivingsprosesser som berører forbrukernes personvern.

9.2 Utviklingstrekk som påvirker forbrukernes personvern

Forbrukerhverdagen har gjennomgått omfattende og grunnleggende endringer i løpet av de siste 20 årene.[12] Stadig større deler av hverdagen har blitt digitalisert. Nordmenn handler varer på nett, forvalter egen økonomi i nettbank, styrer husholdningsapparater med mobiltelefonen, og holder sosial kontakt gjennom sosiale medier. Rundt 96 prosent av alle nordmenn mellom ni og 79 år har smarttelefon.[13] Stadig flere produkter kobles på nett, som bidrar til at mange enheter får nye funksjoner, kan lære av sine omgivelser, og tilby bedre tjenester for forbrukerne.[14]

Digitaliseringen har ikke bare endret *hva* vi forbruker, men også *hvordan* vi forbruker. Innenfor områder som aviser, film, musikk og dataspill har forbruksmønstre beveget seg fra kjøp av fysiske produkter, til forbruk av heldigitale tjenester, ofte i form av abonnementstjenester. Slike tjenester opererer gjerne ved å samle inn data, inkludert personopplysninger, for å skreddersy tjenestetilbud til brukerne og utvikle nye tjenester og produkter.

Den digitale forbrukerhverdagen preges altså av en omfattende datainnsamling om hver enkelt av oss. Mange selskaper vet «alt» om oss, men den enkelte forbruker har hverken kompetanse eller mulighet til å forstå mange av disse selskape-

---

7 Meld. St. 25 (2018–2019) *Framtidas forbrukar - grøn, smart og digital.* Barne- og familiedepartementet.

8 Meld. St. 22 (2020–2021) *Data som ressurs. Datadrevet økonomi og innovasjon.* Kommunal- og moderniseringsdepartementet.

9 Barne- og familedepartementet. (2021). *Rett på nett – Nasjonal strategi for trygg digital oppvekst.*

10 Kommunal- og moderniseringsdepartementet. (2020). *Nasjonal strategi for kunstig intelligens*, s. 56.

11 Kommunal- og moderniseringsdepartementet. (2020). *Nasjonal strategi for kunstig intelligens*, s. 62.

12 Meld. St. 25 (2018–2019) *Framtidas forbrukar – grøn, smart og digital. Barne- og familiedepartementet.*

13 Statistisk Sentralbyrå. (2022). *Norsk mediebarometer 2021.*

14 Statistisk Sentralbyrå. (2021, 20. september). *Netthandelen høyere enn noen gang.*

nes forretningsmodeller, databehandling, eller formål med innsamlingen. Denne informasjonsasymmetrien drøftes videre i avsnitt 9.4.4.

I det følgende gis det en oversikt over digitale tjenester og utviklingstrekk som påvirker forbrukerhverdagen og forbrukernes personvern.

9.2.1 Sosiale medier

Sosiale medier er nettsider og apper som tilrettelegger for å skape og dele innhold, og å samhandle med andre brukere. Sentrale kjennetegn ved sosiale medier er at de ofte eies av globale aktører, og brukes på tvers av landegrenser, samt at de finansieres helt eller delvis av reklame. Facebook er det mest brukte sosiale mediet, med over tre og en halv million brukere i Norge over 18 år. Twitter, Instagram, YouTube, Tiktok og Snapchat er også mye brukt.[15]

Sosiale medier har blitt en hjørnestein i hverdagen. Det er arenaer for å holde kontakt med venner og familie, delta i lokalmiljø og interessefellesskap, følge og delta i samfunnsdebatter, konsumere underholdning, selge og kjøpe produkter, og mye mer. For de fleste forbrukere i Norge er det så godt som umulig å ikke ha noen form for tilstedeværelse i sosiale medier uten at man melder seg ut av samfunnet.

Sosiale medier brukes av privatpersoner til å kommunisere med andre brukere, men de brukes også av virksomheter og organisasjoner til nyhetsformidling, markedsføring, politiske ytringer og offentlig informasjon. Skillet mellom privatpersoner og virksomheter kan fremstå som uklart i sosiale medier. Brukerinnhold og kommersielt innhold kan overlappe, for eksempel ved influensermarkedsføring.

Sosiale medier kjennetegnes ved at forbrukerne kan laste opp, dele, spre og konsumere innhold. I mange tilfeller vil brukerne primært konsumere innhold delt av andre, inkludert av kommersielle eller profesjonelle aktører, heller enn å poste mye selv. I mange sosiale medier skilles det mellom offentlig tilgjengeliggjort innhold, som kan sees av alle brukerne av det sosiale mediet, og privat innhold. Grensedragningen mellom hva som regnes som offentlig tilgjengeliggjort innhold og hva som regnes som privat, kan imidlertid være vanskelig å trekke. Det kan for eksempel være vanskelig å vurdere om en lukket Facebookgruppe med et stort antall medlemmer kan regnes som privat eller offentlig.

[15] Ipsos. (2021). *Sosiale medier tracker Q2'21.*

Boks 9.1 Ida Aalens definisjon av sosiale medier:

«Sosiale medier er et sekkebegrep uten noen anerkjent definisjon, men det er to trekk jeg mener er avgjørende:

For det første finnes det ikke et klart skille mellom avsender og publikum på sosiale medier. De samme menneskene kan både produsere og konsumere.

For det andre legger sosiale medier til rette for mange-til-mange-kommunikasjon.»[1]

[1] Aalen, I. (2019). *Sosiale Medier.* Fagbokforlaget.

Meta, Twitter, Tiktok og andre sosiale medieplattformer har som forretningsmodell å samle inn personopplysninger om brukerne og å utnytte disse videre til markedsføringsformål. Alt fra bruksmønster, lokasjonsdata, interesser, og mer samles inn. Opplysningene brukes til å utvikle annonseverktøy som gjør det mulig for virksomheter og organisasjoner å nå relevante forbrukersegmenter med sitt budskap. For eksempel kan en lokalbedrift som selger fiskeutstyr bruke slike annonseverktøy til å nå forbrukere i nærmiljøet som er opptatt av sportsfiske.

9.2.2 Plattformøkonomien

> *«Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate.»*
>
> *- Tom Goodwin, journalist*[16]

Netthandel har opplevd en betydelig vekst i løpet av de siste ti årene, og har blitt ytterligere forsterket som en følge av covid-19-pandemien.[17] Flere av de største aktørene innenfor netthandel, slik som Amazon, Alibaba og AirBnB, er en del av plattformøkonomien. Plattformøkonomien kjennetegnes av at store, ofte globale plattformer videreformidler salg av varer og tjenester mellom næringsdrivende og forbrukere, eller mellom to

[16] Goodwin, T. (2015, 4. mars). *The Battle Is For The Customer Interface.* Techcrunch.

[17] Finansavisen. (2020, 19. august). *Netthandel til himmels under corona.*

eller flere forbrukere. Flere av de største plattformselskapene selger ikke produkter direkte til forbrukerne, men fungerer som formidlere av produkter og tjenester.

For forbrukerne kan transaksjoner som foregår gjennom plattformer fremstå som alminnelig netthandel. Forbrukeren betaler en sum, og mottar produktet eller tjenesten. Samtidig har dette konsekvenser for kundeforholdet. Er forbrukeren kunde av Uber eller av sjåføren en sitter på med? Hvem har ansvar dersom noe går galt? Dette kan utfordre tradisjonelle forbrukerrettigheter fordi plattformselskapet blir et mellomledd mellom kjøper og selger som ikke var der tidligere.

Plattform-modellen kan ha personvernkonsekvenser for den enkelte dersom plattformen ikke har kontroll over hvordan tredjepartsselgere mottar og behandler personopplysninger. I bakgrunnen samler plattformene selv inn store mengder personopplysninger om forbrukerne, om deres preferanser, brukeranmeldelser og lignende. Denne informasjonen brukes til å tilpasse innhold eller levere en tjeneste. Det er for eksempel nødvendig at en transportplattform vet hvor du befinner deg for å kunne sende en bil til riktig sted.

9.2.3 Oppmerksomhetsøkonomien

Digital markedsføring har blitt hovedinntektskilden for store deler av den digitale økonomien. Digitale annonser lar annonsører og innholdsprodusenter (publisister) målrette budskap, men har også bragt nye muligheter for å måle effekten av markedsføringen. Dette innebærer blant annet kontinuerlig måling av klikk på annonser, hvor mange forbrukere som har sett en annonse, hvor lenge forbrukerne ser på videoer og om en forbruker handlet et produkt etter å ha sett en annonse. Sammen med en økende innsamling av brukerdata, har dette bidratt til fremveksten av en *oppmerksomhetsøkonomi*, hvor forbrukeres oppmerksomhet kvantifiseres og kommersialiseres.

Oppmerksomhetsøkonomien innebærer at plattformer og andre tjenester designes for å holde mest mulig på brukernes oppmerksomhet. Jo mer tid forbrukere bruker på en plattform, jo flere annonser vil de se. Dette vil igjen generere data, som plattformen kan tjene penger på. For eksempel har en rekke strømmeplattformer introdusert automatisk avspilling av videoer, og sosiale medier bruker ofte nyhetsstrømmer som brukeren kan bla gjennom i det uendelige.[18]

I 2021 avslørte en varsler at Facebook promoterte skadelig innhold fordi det skaper brukerengasjement.[19] Avsløringen skapte overskrifter over hele verden, og bekreftet at polariserende og kontroversielt innhold ble prioritert av selskapet fordi det øker inntjeningen.

Det pågår en omfattende samfunnsdebatt om problematiske sider ved sosiale medier og oppmerksomhetsøkonomien generelt. *Personvernkommisjonen* har valgt å avgrense sin drøftelse til de utfordringene som direkte berører personvern.

9.2.4 Tingenes internett

Tingenes internett er et samlebegrep for fysiske produkter som utstyres med programvare, sensorer og andre digitale komponenter. Dette inkluderer alt fra treningsarmbånd og tilkoblede leketøy, til smarthjem og medisinske implantater. Fremveksten av tingenes internett innebærer at personopplysninger kan samles inn på stadig nye måter og i nye kontekster.

Fordelene ved tingenes internett er flerfoldige. Bruken av digital velferdsteknologi som fallsensorer og blodtrykksmålere kan for eksempel bidra til høyere livskvalitet og til at eldre kan bo hjemme lengre. På forbrukersiden kan for eksempel smarthus med stemmeassistenter gjøre hverdagen enklere, mens aktivitetsarmbånd kan motivere til en sunnere livsstil.

Selv om det er flere fordeler ved at stadig flere gjenstander blir internettilkoblede, skaper utviklingen en rekke utfordringer knyttet til personvern og sikkerhet. Svært mange produkter i tingenes internett er utstyrt med sporingsteknologi og sensorer som samler inn informasjon om sine omgivelser. Dette muliggjør datainnsamling i stor skala, og bidrar til at informasjon om bevegelse, kroppslige funksjoner, stemme og mye mer kan registreres, analyseres og gjenbrukes. Problemstillinger knyttet til internettilkoblede produkter diskuteres mer inngående i avsnitt 9.4.1.

9.2.5 Kunstig intelligens

> *«Given the major impact that AI can have on our society and the need to build trust, it is vital that European AI is grounded in our values and fundamental rights such as human dignity and privacy protection.» – Europakommisjonen*[20]

[18] BBC. (2018, 4. juli). *Social media apps are 'deliberately' addictive to users.*

[19] Washington Post. (2021, 26. oktober). *A whistleblower's power: Key takeaways from the FacePapers.*

[20] Europakommisjonen. (2020). *White Paper on Artificial Intelligence – A European approach to exceland trust*, side 2.

Kunstig intelligens (KI) er en samlebetegnelse for maskinlæringssystemer *«som viser intelligent adferd ved å analysere sine omgivelser og utføre handlinger – med en grad av autonomi – for å oppnå gitte mål»*.[21] Et vidt spekter av forbrukerrettede produkter og tjenester inneholder slike maskinlæringssystemer, fra stemmegjenkjenning og søkemotorer til tilkoblede biler. Kunstig intelligens benyttes gjerne for å automatisere prosesser som ellers ville krevd en manuell innsats. For eksempel kan et KI-system brukes for å gjenkjenne ulovlig bildemateriale i et sosialt medium og flagge dette så fort det lastes opp, noe som ville vært fysisk umulig for mennesker å gjennomføre i samme skala.

Siden KI-systemer trenes opp ved å analysere eksisterende data, krever det ofte betydelige mengder opplysninger. Et relativt «enkelt» system, slik som anbefalingssystemene i flere strømmetjenester, fungerer ved at aktivitetsdata fra samtlige brukere samles inn og analyseres i forsøk på å forutse hva en enkelt bruker vil kunne ha interesse av. Dette kan bidra til bedre og mer treffsikre tjenester, samt effektivisering i stor skala, men dersom systemet anvender personopplysninger vil det kunne ha konsekvenser for personvernet til den enkelte forbruker.

Kunstig intelligens kan også anvendes til svært komplekse oppgaver, som legger grunnlaget for nye teknologier. Ansiktsgjenkjenning er et eksempel. Teknologien kan brukes i forbrukerøyemed, for eksempel til å låse opp smarttelefonen ved bruk av telefonens kamera. Ansiktsgjenkjenning kan også brukes for markedsføringsformål. For eksempel møtte Peppes Pizza kritikk i 2017 for å ha brukt denne teknologien i et reklameskilt på Oslo S for å tilpasse markedsføring basert på kjønn.[22]

Kunstig intelligens anvendes også innenfor sektorer som forsikring og finans. For eksempel gjøres kredittvurderinger i mange tilfeller basert på maskinlæringssystemer som analyserer store mengder informasjon for å predikere risiko. Det kan bidra til mer effektiv behandling av søknader, men kan også gjøre det utfordrende å utlede hvorfor en enkeltsøknad blir avvist eller godkjent.

9.2.6 Forbrukernes muligheter til å ivareta eget personvern

I *Personvernkommisjonens* mandat står det at *kommisjonen* skal: «Kartlegge forbrukeres reelle muligheter til å ivareta eget personvern ved bruk av digitale løsninger og tjenester, og vurdere om bransjenormer, merkeordninger eller sertifiseringsmekanismer kan brukes bedre, jf. personvernforordningen kapittel IV avsnitt 5».

Personvernregelverket legger til grunn at registrerte blant annet skal ha mulighet til å kontrollere hvordan egne personopplysninger behandles, hvem opplysningene deles med, og kunne motsette seg behandlingen. I prinsippet har altså forbrukerne rettigheter som skal sikre at deres personvern ivaretas.

I praksis oppfatter imidlertid *Personvernkommisjonen* at mulighetene forbrukerne har til å ivareta eget personvern i dag er svært begrensede. I de følgende avsnittene vil *kommisjonen* beskrive hvordan forbrukerne spores på tvers av tjenester, på nett og i det fysiske rom, av et stort antall aktører de færreste forbrukere har hørt om. Dette har bidratt til at det for de fleste forbrukere er en uoverkommelig oppgave å ha oversikt over, og kontroll med, hvilke opplysninger som samles inn og hvem disse opplysningene deles med. Når data sammenstilles og analyseres for å utlede nye opplysninger, blir det desto vanskeligere å forstå hvordan opplysningene kan anvendes eller misbrukes.

Informasjonsasymmetrien i det digitale forbrukermarkedet kan beskrives som en *systemisk* sårbarhet, hvor markedets struktur fører til at forbrukerne gir opp å forsøke å ivareta personvernet sitt. Dette har ført til at enkelte eksperter innenfor personvern- og forbrukerrett har argumentert for at det bør legges til grunn at *sårbarhet er normaltilstanden* for alle digitale forbrukere, og at alle derfor bør ha rett til ekstra beskyttelse.[23]

For eksempel støter de fleste forbrukere på flere titalls cookieforespørsler på daglig basis. Slike forespørsler dukker opp på de fleste nettsider, og spør om besøkende vil godta bruk av informasjonskapsler (cookies) til en rekke formål. Mengden cookieforespørsler hver enkelt forbruker må ta stilling til hver dag, samt den teknologiske og juridiske kompetansen som er nødvendig for å forstå innholdet i forespørslene, gjør det krevende for de aller fleste å ta et informert valg før man samtykker.

---

[21] Europakommisjonen. (2019). *A definition of Artificial Intelligence: main capabilities and scientific disciplines.*

[22] Dagbladet. (2017, 16. mai). *Reklameskilt ser hvem du er.* DinSide.

[23] Helberger, N., Lynskey, O., Micklitz, H.W., Rott, P., et al. (2021). *EU Consumer Protection 2.0. Structural asym-metries in digital consumer markets.* BEUC.

Mange tjenesteleverandører har tilrettelagt for at brukerne kan tilpasse personverninnstillinger for å ivareta personvernet sitt. Selv om forbrukerne har muligheten til å justere på slike innstillinger, er det få som gjør det, også på de største plattformene.[24] Dette kan skyldes at det er vanskelig å finne fram til og/eller forstå innstillingene, at forbrukerne antar at tjenesteleverandøren ivaretar personvernet, eller at man rett og slett har gitt opp å beskytte eget personvern. Dersom en forbruker tar i bruk personverninnstillinger, er det i mange tilfeller umulig å vite om alle aktørene i verdikjeden respekterer innstillingene som gjøres.[25] I praksis ber man altså hver enkelt forbruker om å gjøre svært kompliserte juridiske og teknologiske vurderinger flere ganger om dagen, kun for å besøke en nettside eller benytte en app.

Det samlede trykket av den kommersielle overvåkning på nett fører altså til at forbrukere i dag har svært liten mulighet til å ivareta eget personvern. Selv om forbrukerne kan endre på enkelte personverninnstillinger, installere programvare som blokkerer enkelte former for sporing, eller velge bort enkelte tjenester, er det i praksis tilnærmet umulig for de aller fleste forbrukere å stanse all potensiell uønsket innsamling og bruk av personopplysninger. Som forklart i kapittel 3, er det også kollektive aspekter ved personvern som ikke kan løses ved individuelle forbrukervalg.

Som følge av at det i dag er begrensede muligheter for den enkelte til å ivareta eget personvern på en effektiv måte, er det i mange tilfeller lite hensiktsmessig å legge ansvaret for ivaretakelse av eget personvern på den enkelte forbruker. Alle tiltak som har til hensikt å styrke forbrukernes evne til selvbeskyttelse, slik som for eksempel nettvett-kampanjer, må derfor ikke sees som en erstatning for regulering og håndheving av eksisterende regelverk.

Personvernkommisjonen ser at forbrukerne i dag har svært begrensede muligheter til å ivareta eget personvern. Samtykkeforespørsler blir brukt i for stor grad, uten å gi noen reell beskyttelse eller kontroll. Dette skaper tretthet og en følelse av avmakt blant forbrukerne. Det er derfor særlig viktig at norske myndigheter tar ansvar for å beskytte norske forbrukeres personvern ved å føre en offensiv personvernpolitikk opp mot EU.

Personvernkommisjonen anbefaler at Regjeringen tar initiativ til å utrede hvordan teknologi kan brukes for å beskytte forbrukere, for eksempel gjennom personvernvennlige standardinnstillinger eller automatisk blokkering av illegitim sporing, som beskrevet i kapittel 11. Det er vesentlig at det offentlige tar et slikt initiativ, slik at det ikke utelukkende er de globale plattformaktørene som i praksis leder an i dette arbeidet.

9.2.6.1 Sertifiseringsmekanismer, atferdsnormer og standarder

Personvernforordningen legger opp til at sertifiseringsmekanismer og atferdsnormer kan anvendes for å styrke personvernet.[26] Slike ordninger kan i prinsippet bidra til at personvernet ivaretas bedre i forbrukertjenester.

Merkeordninger og sertifiseringsmekanismer har imidlertid enkelte svakheter som gjør at de i praksis kan ha begrenset nytteverdi i personvernsammenheng.

Sertifiseringsordninger forutsetter kontinuerlige evalueringer for å sikre reell beskyttelse. Digitale forbrukertjenester er som regel dynamiske, og både funksjonalitet og databehandling kan endres over natten. Det betyr at en tjeneste som er «godkjent»-merket en dag, kan være diskvalifisert til merket neste dag.

Videre er både merkeordninger og sertifiseringsmekanismer som regel frivillige og basert på selvregulering. Dette skaper betydelige utfordringer knyttet til kontroll og etterprøvbarhet. Ettersom mange av de største aktørene opererer globalt, vil det også være vanskelig for en særnorsk ordning å få fotfeste innenfor mange tjeneste- og produktsektorer.

Personvernkommisjonen mener at sertifiseringsmekanismer og bransjenormer kan ha nytteverdi i enkelte tilfeller. Bransjenormer kan for eksempel bidra til å «løfte gulvet» for godt personvern, og gi like forutsetninger for konkurrenter. Nasjonale sertifiseringsmekanismer kan være hensiktsmessige innen sektorer som for eksempel helse eller skole, men det forutsetter kompetansemiljøer som har kontroll med hvilke systemer som anskaffes og iverksettes, og ansvar for å kontinuerlig følge opp at sertifiseringen er i tråd med den faktiske databehandlingen.

Personvernkommisjonen mener videre at internasjonalt standardiseringsarbeid kan bidra til at produkter og tjenester med høy personvernrisiko ikke selges hos norske forhandlere. Dette forut-

[24] Inc. (2020, 31. juli). *Google Just Revealed How Many People Use Its Privacy Checkup Tool. It's Not Good News.*

[25] Cnet. (2019, 14. februar). *These Android apps have been tracking you, even when you say stop.*

[26] Personvernforordningen artikkel 40 og 42.

setter imidlertid at det internasjonale standardarbeidet foregår i åpne og demokratiske prosesser, hvor aktører og representanter fra for eksempel sivilsamfunnet kan delta på lik linje med bransjeorganisasjoner og store teknologiselskaper.[27]

9.3 Rettslige rammer

Behandling av forbrukeres personopplysninger omfattes av personvernregelverket, se omtale av personvernregelverkets materielle virkeområde i kapittel 4. Det betyr at regelverkets krav til behandlingsansvarlige og de registrertes rettigheter gjelder når næringsdrivende behandler forbrukeres personopplysninger.

Utover personvernregelverket reguleres behandling av forbrukeres personopplysninger av både nasjonal og internasjonal lovgivning.

Digitale tjenester er underlagt en rekke ulike reguleringer. Særlovgivning som for eksempel gjelder for kjøp og salg av bolig, skiller seg fra regelverk som gjelder apper som tilbyr kjøp og salg av fond.

En ytterligere kompliserende faktor er at mange nye og innovative digitale forbrukertjenester utfordrer det etablerte regelverket, som ofte er utviklet for å regulere analoge arbeidsprosesser eller tjenester. Dette medfører at det oppstår en mengde gråsoner og tolkningsmuligheter som gjør det vanskelig for digitale forbrukere (og til en viss grad også for tjenesteleverandører) å forstå og å hevde rettighetene sine.

Nedenfor gjøres det kort rede for relevant sektorlovgivning. Dette etterfølges av en kortfattet oversikt over kommende nye regelverk som vil ha relevans for norske forbrukeres personvern.

9.3.1 Sektorlovgivning

Forbrukernes forhold til digitale tjenesteleverandører reguleres gjennom en rekke lover, inkludert blant annet markedsføringsloven, angrerettloven og forbrukerkjøpsloven. Disse lovene berører ikke personvernspørsmål direkte, men er i flere tilfeller tilstøtende til personvernregelverket, for eksempel når det gjelder atferdsbasert markedsføring.

Markedsføringsloven og forbrukerkjøpsloven håndheves av Forbrukertilsynet. Markedsføringsloven regulerer markedsføring mot forbrukere, samt forbud mot urimelige avtalevilkår i kontrakter som inngås mellom forbruker og næringsdrivende. Et av lovens mest sentrale avsnitt gjelder forbud mot villedende og urimelig handelspraksis. Det inkluderer blant annet forbud mot aggressiv og villedende markedsføring.[28] Barn har et særlig krav på vern etter markedsføringsloven, som beskrives nedenfor i avsnitt 9.5. Forbrukerkjøpsloven regulerer forholdet mellom næringsdrivende og forbruker. Loven gir blant annet regler for vareoverlevering ved et salg, og gir rammer for hva som kan inkluderes i en kjøps- og salgskontrakt.[29]

9.3.1.1 Særnorsk implementering av kommunikasjonsvernsdirektivet

Lov om elektronisk kommunikasjon (ekomloven) håndheves av Nasjonal kommunikasjonsmyndighet. Ekomloven med forskrifter regulerer blant annet kommunikasjonsvernet, herunder taushetsplikt for tilbydere med mer, sletteplikt for trafikkdata mv., samt krav til vern av kommunikasjon og data. Hensynet bak kommunikasjonsvernet er langt på vei sammenfallende med formålet med personvernet. Ekomloven inneholder også bestemmelser og krav for bruk av informasjonskapsler (cookies) og annen sporingsteknologi, som følger av norsk implementering av kommunikasjonsvernsdirektivet.[30] Europakommisjonen la fram et forslag om en kommunikasjonsvernforordning i 2017, men det er ikke klart når en slik forordning vil bli vedtatt.

Kommunikasjonsvernsdirektivet regulerer blant annet personvernet i kommunikasjonsutstyr, og gjelder dersom sporingsteknologi plasseres på sluttbrukerutstyr. Det betyr at lagring av eller uthenting av opplysninger fra en datamaskin eller telefon, som ikke er nødvendig for å levere en tjeneste, reguleres av ekomloven. Videre behandling av personopplysninger som eventuelt samles inn gjennom teknologien vil falle inn under personopplysningsloven. I praksis betyr dette at Nasjonal kommunikasjonsmyndighet har ansvar for å håndheve reglene knyttet til plassering av informasjonskapsler, mens Datatilsynet har ansvar for håndheving av etterfølgende behandling av personopplysninger.

---

27 ANEC. (u.å). *The Standardisation Regulation.*

28 Lov 9. januar 2009 nr. 2 om kontroll med markedsføring og avtalevilkår (markedsføringsloven).

29 Lov 21. juni 2002 nr. 34 om forbrukerkjøp (forbrukerkjøpsloven).

30 Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon. (Kommunikasjonsverndirektivet). Kommunikasjonsverndirektivet er gjennomført i norsk rett i ekomloven..

I flere andre land i Europa er det datatilsynene som har ansvar for å håndheve bestemmelsene i kommunikasjonsvernsdirektivet, inkludert bruken av informasjonskapsler. Mens det i disse landene foreligger krav om at bruk av informasjonskapsler krever et samtykke i tråd med personopplysningsloven, har direktivet i Norge blitt gjennomført på en måte som gjør at forhåndsinnstillinger i nettleser kan ansees som et gyldig samtykke. Det betyr i praksis at det i Norge ikke foreligger et krav om samtykke i tråd med personvernforordningen for å plassere informasjonskapsler på sluttbrukerutstyr.

I 2021 var forslag til ny ekomlov ute på høring, og i den forbindelse foreslo blant annet Datatilsynet og Forbrukertilsynet at loven endres slik at bestemmelsene om informasjonskapsler samsvarer med resten av Europa, og at ansvaret for å håndheve bruk av informasjonskapsler og annen sporingsteknologi flyttes fra Nasjonal kommunikasjonsmyndighet til Datatilsynet for å sikre en helhetlig tilnærming til sporing på nett.[31]

Personvernkommisjonen anbefaler at ansvaret for håndheving av bruk av informasjonskapsler og lignende sporingsteknologi legges til Datatilsynet.

Personvernkommisjonen mener Regjeringen bør støtte et forslag om en kommunikasjonsvernforordning som stiller krav til bruk av sporingsteknologi som er i samsvar med personvernforordningen.

9.3.2 Kommende europeisk regulering

Det arbeides fortløpende med ny regulering på EU-nivå for å harmonisere eksisterende regelverk, samt for å sørge for at europeiske forbrukeres rettigheter ivaretas i møte med digitaliseringen. Nedenfor gjøres det kort rede for lovprosesser som er særlig relevante for forbrukeres personvern.

9.3.2.1 Digitalytelsesloven

I 2019 vedtok EU et direktiv for å gjøre det enklere for forbrukere og næringsdrivende å inngå forbrukeravtaler på tvers av medlemsstatenes landegrenser.[32] Direktivet kommer til anvendelse på avtaler der forbrukeren påtar seg «at betale en pris», men også der forbrukeren avgir personopplysninger i stedet for å betale med penger. Direktivet gjennomføres i norsk lov gjennom ny lov om levering av digitale ytelser til forbrukere (digitalytelsesloven). Loven ble vedtatt av Stortinget i juni 2022, og trer i kraft 1. januar 2023. Av høringsnotatet som lå til grunn for forslaget fremkommer det at loven skal gjelde «avtaler om levering av digitale ytelser mot vederlag i forbrukerforhold».[33] Videre følger det av høringsnotatet at direktivet ikke bare skal omfatte «avtaler der det ytes et tradisjonelt vederlag i form av penger, men også avtaler der vederlaget består i å oppgi visse personopplysninger, jf. artikkel 3 nr. 1.»[34]

9.3.2.2 Forordning om digitale ytelser og om digitale markeder

Forordningen om digitale ytelser (Digital Services Act, DSA) og forordningen om digitale markeder (Digital Markets Act, DMA) har som formål å regulere digitale plattformer av forskjellig størrelsesorden. DMA ble endelig vedtatt av Rådet 18. juli 2022. DSA er foreløpig på forslagsstadiet, men det forventes at forordningen blir endelig vedtatt i Rådet i løpet av september 2022. Begge forordningene forventes iverksatt i begynnelsen av 2024.

DSA er blant annet en oppdatering av e-handelsdirektivet, og har som et av sine hovedformål å utjevne maktubalansen mellom forbrukere og digitale tjenesteleverandører. Forordningen skal gi forbrukere bedre beskyttelse ved blant annet å sikre informasjon, tilgang på tvisteløsningsmekanismer og gjennomsiktige vilkår og betingelser, og introduserer en rekke bestemmelser knyttet til blant annet digital markedsføring og manipulasjon.[35] Forordningen erstatter nasjonale regler slik at praksis blir enhetlig i hele EU. Siden forslaget til DSA ikke er formelt vedtatt enda, er det heller ikke tatt endelig stilling til om forordningen er EØS-relevant.[36]

Utkastet til DSA omfatter alle internettbaserte tjenesteleverandører som tilbyr tjenester innenfor

---

31 Datatilsynet og Forbrukertilsynet. (2021). *Felles høringssvar fra Forbrukertilsynet og Datatilsynet – Forslag til ny ekomlov § 3-7 – samtykke til informasjonskapsler.*

32 Justis- og beredskapsdepartementet. (2021). *Høringsnotat – ny lov om levering av digitale ytelser til forbrukere (digitalytelsesloven)*, side 4.

33 Justis- og beredskapsdepartementet. (2021). *Høringsnotat – ny lov om levering av digitale ytelser til forbrukere (digitalytelsesloven)*, side 80.

34 Justis- og beredskapsdepartementet. (2021). *Høringsnotat – ny lov om levering av digitale ytelser til forbrukere (digitalytelsesloven)*, side 4.

35 Europaparlamentet. (2022, 20. januar). Digital Services Act: regulating platforms for a safer online space for users.

36 Forordningsforslaget til DSA ble presentert av Europakommisjonen i desember 2020. 23. april 2022 ble det oppnådd enighet mellom Europaparlamentet og Rådet om en endelig avtaletekst. Europaparlamentet vedtok den endelige teksten 5. juli 2022. Forordningsforslaget er pr 1. juli 2022 foreløpig ikke endelig godkjent i Rådet.

EU, uavhengig av om de er basert i eller utenfor EU. Forslaget til forordning retter seg mot en rekke ulike typer plattformer på internett, fra tekniske tjenestetilbydere (ISPer), domeneregistrarer og tilbydere av webhoteller og skytjenester, til markedsplasser, store søkemotorer og sosiale medier. Det stilles ekstra strenge krav til det som i DSA defineres som veldig store søkemotorer og plattformer, det vil si de som har mer enn 45 millioner aktive månedlige brukere i EU.

Forordningsforslaget omhandler ikke direkte personopplysninger, men vil stille ytterligere krav til internettbaserte digitale tjenester. Krav som gjennomsiktighet, risikostyring, og forpliktelser rundt sporing av brukere vil kunne bidra til å styrke personvernet til forbrukere.

DMA er først og fremst rettet mot de største plattformene på internett, såkalte «portvoktere». Forordningen har som formål å styrke konkurransen i digitale markeder ved å motvirke maktubalansen mellom de største tjenesteleverandørene og mindre aktører. Det vil blant annet inkludere en kravliste som må følges av de aller største aktørene, forbud mot noen typer konkurransehemmende praksis for disse aktørene, og andre konkurransefremmende elementer.

DMA vil bare gjelde plattformselskaper med en verdi på minst 75 milliarder euro eller årlig omsetning på 7,5 milliarder euro, som tilbyr noen spesifiserte digitale tjenester (for eksempel meldingstjenester, nettlesere, sosiale medier), og som har minimum 45 millioner brukere hver måned i EU eller 10 000 profesjonelle brukere i året.

9.3.2.3 Forordning for kunstig intelligens

EU arbeider for tiden med en ny forordning for å regulere kunstig intelligens (KI). Denne forordningen vil blant annet gjelde enkelte KI-systemer som anvendes av eller brukes mot forbrukere. Forordningen forventes å tre i kraft i perioden mellom 2022 og 2024.[37]

Forslaget til KI-forordning har en risikobasert tilnærming, med inndeling i risikokategorier. Det er foreslått at forordningen vil forby enkelte anvendelser av kunstig intelligens som innebærer uakseptabel risiko for personers trygghet og rettigheter, samt stille strenge krav for KI-systemer som ansees som høyrisiko.[38] Anvendelse av kunstig intelligens som vil kunne anses å innebære uakseptabel risiko, og som det dermed er foreslått forbud mot, inkluderer blant annet «subliminale teknikker», enkelte former for biometri, myndigheters bruk av sosial scoring og andre anvendelser som utnytter sårbarheter.

KI-forordningen er foreslått supplert med en rekke vedlegg, som vil kunne oppdateres etter hvert som teknologien utvikles og nye utfordringer oppstår. Blant annet beskriver vedlegg I hvilke former for teknologi som er foreslått omfattet av forordningens KI-begrep, mens vedlegg III beskriver hvilke anvendelser av KI-systemer som regnes som høyrisiko. Bruk som anses som høyrisiko er blant annet foreslått å være bruk av kunstig intelligens for biometrisk identifisering og kategorisering, bruk av kunstig intelligens i ansettelser og innenfor utdanning, rettsvesenet, velferdstjenester, politiarbeid, samt for grensekontrollformål.

Systemer som anses som høyrisiko er foreslått å være underlagt strenge krav før de kan plasseres på markedet, inkludert krav om risikovurderinger, krav om høy grad av sikkerhet og nøyaktighet, gjennomsiktighet og forklarbarhet, blant annet gjennom dokumentasjonskrav for å muliggjøre tilsyn. All bruk av systemer for biometrisk fjernidentifisering er foreslått å utgjøre høyrisiko. Som beskrevet i kapittel 5, kan bruk av biometrisk fjernidentifikasjon i det offentlige rom i praksis ville bli forbudt. Det vil likevel kunne være enkelte unntak for terrorbekjempelse, søken etter savnede barn, samt for å identifisere mistenkte i seriøse straffesaker.[39]

I sitt høringsinnspill til Europakommisjonens utkast til KI-forordning peker Kommunal- og distriktsdepartementet blant annet på at forordningen bør omfatte systemer som fører til økonomiske skadevirkninger, for å beskytte forbrukere.[40] En rekke organisasjoner fra sivilsamfunnet rundt om i Europa har kritisert forslaget til KI-forordning for å ha en for snever definisjon av KI-systemer, samt at forslaget ikke introduserer rettigheter for personer som påvirkes av KI-systemer.[41] Andre har påpekt at forslaget til forordning har svakheter knyttet til en for snever definisjon av skadevirkninger, samt at forslaget kun gjelder utviklere

---

37 Europakommisjonen. (2022). *Regulatory framework proposal on artificial intelligence.*

38 Europakommisjonen. (2022). *Regulatory framework proposal on artificial intelligence.*

39 Europakommisjonen. (2022). *Regulatory framework proposal on artificial intelligence.*

40 Kommunal- og distriktsdepartementet. (2021). *Norwegian Position Paper on the European Commission's Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending CerUnion Legislative Acts (COM(2021) 206)*. Europakommisjonen.

41 Access Now. (2021, 30. november). *The EU needs an Artificial Intelligence Act that protects fundamental rights.*

av KI-systemer, og dermed kan skape smutthull for de som anvender systemene.[42] Det er også utfordringer ved at forslaget overlater et stort ansvar til internasjonale standardiseringsprosesser, som ofte er drevet fram av private næringslivsaktører som forordningen skal regulere.[43]

Personvernkommisjonen anbefaler at Regjeringen engasjerer seg i utformingen av forordningen for kunstig intelligens med vedlegg, og jobber for en regulering som sørger for at KI-systemer utformes på en måte som ivaretar personvernet i både utvikling og bruk av systemene.

9.3.2.4 Regulering av informasjonssikkerhet

EU er også i gang med å iverksette nye regelverk som blant annet har som formål å styrke personvern og sikkerhet i tilkoblede forbrukerprodukter. Europakommisjonen vedtok i 2021 å oppdatere Radioutstyrsdirektivet, som regulerer bruk av trådløst utstyr, til å omfatte forbrukerprodukter, blant annet med hensikt om å sikre personvernet.[44] Denne lovendringen forventes å tre i kraft i 2024. Europakommisjonen har også kunngjort en ny strategi for IKT-sikkerhet, Cyber Resilience Act. Denne rettsakten har som et av sine formål å stadfeste strengere sikkerhetsregler og standarder for tilkoblede produkter.[45]

Personvernkommisjonen anbefaler at Regjeringen støtter Europakommisjonens forslag om en horisontal IKT-sikkerhetslov (Cyber Resilience Act).

9.4 Personvernutfordringer og konsekvenser

Ivaretakelse av personvernet er en viktig forutsetning for at den enkelte skal kunne utøve forbrukermakt og ta gode og informerte valg. Ivaretakelse av personvernet er slik sett nært knyttet til ivaretakelse av forbrukerrettigheter. I dette kapitlet fokuserer *Personvernkommisjonen* primært på hvordan forbrukernes personvern settes under press som følge av det digitale skiftet, og hvilke konsekvenser dette har.

Digitaliseringen av forbrukerhverdagen har bidratt til at stort sett alt forbrukerne foretar seg er gjenstand for registrering og innsamling – alt blir omgjort til data. Personopplysninger brukes til alt fra produkt- og tjenesteutvikling til analyse, markedsføring og personalisering. I mange tilfeller tilbys forbrukertjenester «gratis» fordi tjenestetilbyderen baserer sin forretningsmodell på bruk og analyse av personopplysninger – ofte med markedsføring som hovedformål. I noen tilfeller kan alternativet være at forbrukerne må betale med penger for å bruke tjenesten. Mange tjenesteleverandører har kommersiell utnyttelse av personopplysninger som en ekstra inntektsstrøm, også i tilfeller der forbrukerne har betalt for produktet eller tjenesten.

Fremveksten av denne forretningsmodellen har bidratt til et sterkt insentiv til å samle inn mest mulig informasjon om forbrukerne. Tjenestetilbydere som tjener penger på innsamling, bruk og salg av personopplysninger har en egeninteresse i at forbrukerne deler så mange personopplysninger som mulig, eller at de samtykker til datainnsamlingen og til vide formål med databehandlingen.

Utviklingen av kraftigere teknologi for innsamling, lagring og behandling av data har ført til at virksomheter kan samle inn og bruke informasjon som tidligere ikke var anvendelig på grunn av struktur og mengde. Alt fra forsikringsselskaper til tannbørsteprodusenter har enten begynt, eller intensivert, innsamlingen av kundedata.[46] Denne trenden fører til innovasjon og tjenesteutvikling som kommer forbrukerne til gode, men den bidrar også til at mange selskaper opparbeider seg omfattende kunnskap og innsikt om forbrukerne og deres interesser og preferanser.

Det ligger mye makt i å ha omfattende kunnskap om og innsikt i den enkelte forbrukers vaner og interesser. For den enkelte kan det være utfordrende å ha kontroll og oversikt over hva selskapene vet og hvordan denne kunnskapen brukes. Fremveksten av forretningsmodeller basert på innsamling av personopplysninger har derfor blitt møtt med kritikk fra blant annet menneskerettighetsorganisasjoner, forbrukerorganisasjoner og akademikere. Amnesty International har for eksempel uttalt at forretningsmodellene til Alphabet og Meta utgjør en trussel for flere grunnleggende menneskerettigheter.[47]

---

42 Veale, M. & Borgesius, F.Z. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International, 22*(4), 97-112.

43 Helberger, N., Micklitz, H.W. & Rott, P. (2021). *The Regulatory Gap: Consumer Protection in the Digital Economy.* BEUC.

44 Europakommisjonen. (2021, 29. oktober). *Commission strengthens cybersecurity of wireless devices and products.*

45 Breton, T. (2021, 16. september). *How a European Cyber Resilience Act will help protect Europe.* Europakommisjonen.

46 Christl, W. (2017, 2. juni). *Corporate Surveillance in Everyday Life. Crackedlabs.*

9.4.1 Tingenes internett muliggjør sporing overalt

Fremveksten av tingenes internett har ført til at forbrukere kan spores i stadig større grad når de beveger seg rundt i fysiske omgivelser. Produksjonen og utviklingen av internettilkoblende produkter blir stadig billigere. Dette fører til at markedet preges av mange aktører som mangler kompetanse eller vilje til å utvikle personvernvennlige løsninger.

I Norge har Forbrukerrådet avdekket at enkelte tilkoblede leker og smartklokker for barn mangler helt grunnleggende sikkerhets- og personverntiltak. I enkelte av produktene var det blant annet mulig for utenforstående å få tilgang til, og kontroll over, produktet med enkle grep.[48] Å avdekke slike mangler krever som regel høy teknisk kompetanse. En vanlig forbruker har derfor få muligheter til å kunne kontrollere om grunnleggende sikkerhets- og personvernfunksjoner er på plass i tilkoblede produkter.

En befolkningsundersøkelse gjennomført på vegne av Forbrukerrådet i 2019, viste at tre av fire forbrukere var bekymret for at tilkoblede produkter samlet inn mer informasjon enn de hadde samtykket til.[49] Denne mangelen på tillit kan legge en demper på utbredelsen av verdifull teknologi, ved at forbrukere kan vegre seg for å ta produkter som kan øke livskvaliteten deres i bruk.

I USA blir det stadig vanligere at data fra for eksempel treningsarmbånd benyttes i forsikringsøyemed.[50] Slik kan forbrukere med en sunn livsstil «premieres» med lavere forsikringspremier og lignende. I Norge har lignende tiltak vært brukt i bilforsikringsbransjen, hvor sensorer i bilen registrerer kjøremønster for å påvirke forsikringspremien.[51] Slike løsninger kan bidra til tryggere kjøremønster eller sunnere livsstil, men skaper også nye utfordringer. For eksempel kan utviklingen føre til at de som ikke lar seg overvåke må betale mer for forsikringen, og individualiserte forsikringer kan undergrave prinsippet om risikodeling.[52]

Boks 9.2 Stalkerware

«Stalkerware» er et samlebegrep for digitale løsninger som gjør det mulig å overvåke andres privatliv gjennom telefonen, for eksempel ved å gi en sjalu partner tilgang på partnerens lokasjon eller meldinger.[1] Slik bruk kan være enten tilsiktet fra leverandøren, eller oppstå som et følge av manglende risikovurderinger i produktutviklingen. For eksempel møtte Apple kritikk da de lanserte produktet AirTags, små sporingsbrikker som skulle gjøre det enklere for forbrukere å holde styr på nøkler, bagasje og lignende. Brikkene viste seg også å være velegnet til å spore personer uten at de la merke til det, og Apple hadde ikke bygget inn tilstrekkelige sikkerhetsmekanismer for å forhindre slik misbruk av teknologien.[2]

1 Coalition Against Stalkerware. (u.å). *What is stalkerware.*

2 BBC. (2022, 20. januar). *Apple AirTags – A perfect tool for stalking.*

Bruken av sensorer skaper også personvernutfordringer når det benyttes i butikker og kjøpesentre. Datatilsynet har kartlagt hvordan virksomheter sporer forbrukerne ved hjelp av forskjellige sensorer når de beveger seg rundt i det offentlige rom. Formålet med sporingen er i hovedsak å kartlegge atferdsmønstre for kommersielle formål.[53] Det er vanskelig for den enkelte å reservere seg mot slik sporing da virksomheter ofte ikke informerer, eller informerer på en hensiktsmessig måte, om at denne teknologien benyttes.

Inntoget av tilkoblede produkter i private hjem reiser også en rekke spørsmål knyttet til innsamling av personopplysninger. Kan middagsbesøket, for eksempel, motsette seg at opplysninger om dem samles inn og behandles når samtaler fanges opp av stemmeassistenten i stua og sendes til smarthusleverandøren, samt i noen tilfeller også en rekke tredjepartsselskaper?

47 Amnesty International. (2019, 21. november). *Surveillance giants: How the business model of Google and Facebook threatens human rights.*

48 Forbrukerrådet. (u.å). *Tingenes Internett.*

49 Forbrukerrådet. (2019, 15. mars). *Forbrukere stoler ikke på smarte produkter.*

50 The Verge. (2018, 26. september). *What happens when life insurance companies track fitdata?*

51 NRK. (2017, 5. mai). *Tilbyr rimeligere bilforsikring hvis du lar deg overvåke.*

52 Datatilsynet. (2018). *Personlige finanser. Hvordan utviklingstrekk i finanssektoren påvirker personvernet.*

53 Datatilsynet. (2016). *Sporing i det offentlige rom.*

Det er uklart i hvilken grad importører og forhandlere av tilkoblene produkter kontrollerer eller stiller krav til produsentene for å sikre at de overholder kravene i personvernregelverket. Det er svært problematisk at norske forhandlere selger produkter som ikke ivaretar forbrukernes personvern.

Personvernkommisjonen understreker viktigheten av at utviklere og produsenter av digitale forbrukerprodukter og tjenester gjør grundige personvernkonsekvensvurderinger for forskjellige bruksscenarier, særlig med tanke på hvordan tjenester og produkter kan misbrukes.

Personvernkommisjonen anbefaler at norske importører, forhandlere og bransjeorganisasjoner har informasjon tilgjengelig om hvordan personvernet ivaretas før salg av tilkoblede produkter.

Personvernkommisjonen anbefaler at forhandlere har kontrollrutiner på plass for å sikre at produkter som selges i Norge opererer i tråd med personvernforordningen og ekomloven, og stiller krav til sine leverandører knyttet til blant annet dataminimering, formålsbegrensning og personvern som grunninnstilling. Bransjestandarder og merkeordninger kan være et viktig verktøy for å sørge for at leverandørene ivaretar slike krav.

Personvernkommisjonen anbefaler at Regjeringen har som posisjon i regelverksutvikling at forhandlere får et rettslig ansvar for manglende IKT-sikkerhet og personvern i produkter de selger.

9.4.2 Illegitim sporing og profilering

De omfattende mengdene med personopplysninger som samles inn om forbrukerne når de benytter ulike digitale tjenester, benyttes i mange tilfeller til å bygge profiler av den enkelte, eller til å sortere forbrukere i kategorier og segmenter. Profiler kan være bygget på opplysninger om demografi (kjønn, aldersgruppe), handlingsmønster (netthistorikk, lokasjonsmønster, betalingshistorikk), antagelser om personlighetstrekk («impulsiv», «forsiktig»), metadata (identifikatorer, skjermstørrelse) og mye mer.[54] Profilering defineres i personvernforordningen som «enhver form for automatisert behandling av personopplysninger som innebærer å bruke personopplysninger for å vurdere visse personlige aspekter knyttet til en fysisk person, særlig for å analysere eller forutsi aspekter som gjelder nevnte fysiske persons arbeidsprestasjoner, økonomiske situasjon, helse, personlige preferanser, interesser, pålitelighet, atferd, plassering eller bevegelse».[55]

Profilering kan anvendes til en rekke legitime formål, for eksempel til å tilby skreddersydde tjenester som musikkanbefalinger basert på interesser og preferanser. Profilering kan imidlertid også bidra til å urettmessig forskjellsbehandle forbrukere, som ved at enkelte forbrukere får høyere priser enn andre fordi de er regnet som impulsive, eller ved at sårbarheter utnyttes for økonomisk gevinst. Slik bruk av profilering omtales nærmere i avsnitt 9.4.5 om diskriminering og manipulering.

Det eksisterer en hel bransje med aktører som livnærer seg på å samle inn personopplysninger og bygge omfattende profiler, såkalte *datameglere*. Datameglerbransjen henter inn informasjon om forbrukere gjennom forskjellige sporingsteknologier, samt fra andre aktører, offentlige registre, og en rekke andre kilder.[56]

Opplysningene som samles inn av datameglere og lignende foretak brukes hovedsakelig til markedsføringsformål. Forbrukerne kategoriseres med utgangspunkt i profilene og plasseres i segmenter som selges videre til markedsførere og annonsører som ønsker å nå bestemte målgrupper med annonser for sine produkter. Tanken er at jo mer informasjon man har om en forbruker, dess lettere vil vedkommende være å nå med relevante budskap.

Selv om innsamlingen av personopplysninger som foregår på internett i hovedsak skjer med hensikt om å målrette markedsføring, brukes informasjonen som samles inn også til andre formål. Det finnes en rekke eksempler på at datameglere har solgt informasjon til aktører som har helt andre formål.[57] I en rapport fra NATOs Strategic Communications Centre of Excellence advares det om at datameglerindustrien utgjør en trussel for nasjonal sikkerhet, på grunn av mengden informasjon som samles inn om enkeltindivider.[58]

I Norge har blant annet Amnesty International Norge, Datatilsynet, Forbrukerrådet og Teknologirådet foreslått at det de kaller *overvåkningsbasert markedsføring* forbys i sin helhet.[59] Organisasjonene argumenterer blant annet for at denne for-

---

54 Christl, W. (2017). *How Companies Use Personal Data Against People.* Cracked Labs.

55 Personvernforordningen art. 4 nr. 4.

56 Datatilsynet. (2015). *Det store datakappløpet.*

57 Vox. (2020, 2. desember). *A surprising number of government agencies buy celllocation data. Lawmakers want to know why.*

58 Twetman, H., & Bergmanis-Korats, G. (2021). *Data Brokers and Security.* Riga: NATO Strategic Communications Centre of Excellence.

59 Thon, B.E., Blyverket, I.E. & Egenæs, J.P. (2021, 21. oktober). *Nok er nok! Gigantene må tøyles.* Aftenposten.

men for markedsføring, som baserer seg på sporing og profilering av forbrukere, bryter med grunnleggende forbrukervern, personvern og menneskerettigheter.

En gruppe europaparlamentarikere har tatt til orde for et lignende forbud gjennom alliansen Tracking-Free Ads Coalition.[60] Forbrukerrådet har også publisert et opprop for et forbud sammen med over 50 forbruker- og digitale rettighetsorganisasjoner i Europa og USA.[61]

I Norge har blant annet norske mediebedrifter, gjennom Mediebedriftenes Landsforening (MBL), hatt dialog med Datatilsynet knyttet til hvordan atferdsbasert markedsføring kan gjøres på en lovlig og forsvarlig måte. Mediebedriftene i MBL benytter målrettet annonsering til å finansiere fri, uavhengig journalistikk. MBL har etablert regler knyttet til atferdsbasert markedsføring. Blant annet har mediebedriftene i MBL innført et selvpålagt forbud mot å benytte personopplysninger som gjelder barn og særlige kategorier av personopplysninger. Det er også inntatt begrensinger knyttet til bruk av detaljerte lokasjonsdata og fastsatt begrensede lagringstider. Mediebedriftene kan kun benytte egne såkalte førstepartsdata til markedsføringsformål og det er ikke lov for tredjepartsaktører å samle inn opplysninger om brukerne til å bygge og berike sine egne profiler. Dette forbudet følges opp gjennom juridisk og teknisk revisjon av tredjepartene.[62]

Personvernkommisjonen anser at store deler av det digitale annonsesystemet i dag er ute av kontroll, hvor en betydelig innsamling og deling av personopplysninger til potensielt tusenvis av selskaper skjer i sanntid hver eneste dag. Disse opplysningene brukes blant annet til å lage digitale profiler, som igjen kan brukes til å målrette budskap, til og med mot mennesker i sårbare livssituasjoner. Dette fører til diskriminering, manipulasjon, at privat informasjon kommer på avveie, sikkerhetsutfordringer, nedkjølingseffekter og mer.

Europaparlamentet har foreslått å forby atferdsbasert markedsføring mot barn som en del av forordningen om digitale tjenester (DSA), samt å forby bruken av særlige kategorier av personopplysninger til markedsføringsformål.[63]

I Norge har Regjeringen støttet forbudet mot atferdsbasert markedsføring rettet mot barn som er foreslått som en del av DSA. Dette begrunnes med at barn og unge er en sårbar gruppe med særlig behov for beskyttelse.[64]

Personvernkommisjonen deler Regjeringens syn på at atferdsbasert markedsføring mot barn bør forbys. *Kommisjonen* støtter også at bruken av særlige kategorier av personopplysninger til markedsføringsformål forbys. Forbudet bør også gjelde særlige kategorier av personopplysninger som er utledet fra data som ikke var sensitive ved innsamlingspunktet, for eksempel lokasjonsdata som sammenstilt kan avdekke politisk eller religiøs tilhørighet.

Personvernkommisjonen anbefaler at ved et forbud mot atferdsbasert markedsføring som kun gjelder barn, må tjenesteleverandører pålegges et føre var-prinsipp. Det er ikke ønskelig med løsninger som fører til økt sporing og profilering for å kartlegge forbrukeres identitet og alder. *Personvernkommisjonen* anbefaler videre at ikke bare atferdsbasert markedsføring *mot* barn forbys, men også at *bruk av* barns personopplysninger til atferdsbasert markedsføring bør forbys. Barns personopplysninger bør ikke anvendes til atferdsbasert markedsføring, selv om markedsføringen ikke rettes mot barn.

Personvernkommisjonen har delt seg i et flertall og et mindretall i spørsmålet om et *generelt forbud* mot atferdsbasert markedsføring bør utredes.

Personvernkommisjonens flertall, medlemmene Busch, Grande, Haugli, Hertzberg, Høyer, Myrstad, Schartum, Veum, Ytre-Arne og Aasberg, ønsker å fremheve at atferdsbasert markedsføring også kan være skadelig for befolkningen for øvrig. Av den grunn mener *kommisjonens flertall* at det bør utredes hvorvidt et generelt forbud er nødvendig for å beskytte norske og europeiske forbrukere. En slik utredning bør se på hvilke positive og negative konsekvenser et slikt forbud vil ha i Norge og i Europa, blant annet for medieindustrien. Digital markedsføring er i dag en vesentlig kilde til å finansiere fri, uavhengig journalistikk.

Dissens fra kommisjonsmedlemmene Moen og Næss:

Personvernkommisjonens mindretall, medlemmene Moen og Næss anser at atferdsbasert annonsering kan gjøres på ulike måter – forsvarlig og uforsvarlig. Medlemmene Moen og Næss mener at så

60 Tracking-Free Ads Coalition. (u.å). *Supporters.*

61 Forbrukerrådet. (2021, 22. juni). *International coalition calls for action against surveillance-based advertising.*

62 Mediebedriftenes Landsforening. (2021, 17. november). *Notat vedrørende MBLs posisjon og innspill til det pågående arbeid i EU om regulering av målrettet annonsering.*

63 Politico. (2022, 20. januar). *European Parliament pushes to ban targeted ads based on health, religion or sexual orientation.*

64 Kommunal- og distriktsdeparte & Barne- og familiedepartementet (2022, 28. februar). *Norge ønsker forbud mot adferdsbasert markedsføring mot barn og unge på nett.*

lenge atferdsbasert markedsføring gjøres forsvarlig vil et generelt forbud være uforholdsmessig. *Moen og Næss støtter derfor ikke flertallets forslag om at det bør utredes hvorvidt et generelt forbud er nødvendig.*

Moen og Næss ser med uro på et eventuelt forbud mot atferdsbasert annonsering generelt. Et generelt forbud mot atferdsbasert markedsføring vil i praksis ramme mediene hardt, og ramme en helt avgjørende finansieringskilde for å sikre at kvalitetsjournalistikk er tilgjengelig for flest mulig. Moen og Næss mener det er fullt mulig, og nødvendig, å ha en ansvarlig tilnærming til bruk av data i annonsemarkedet – og at et totalforbud rammer både aktører med et mer omtrentlig forhold til personvern og aktører som tar sitt ansvar på dypeste alvor.

Moen og Næss anser videre at det er utfordringer knyttet til hvordan man definerer atferdsbasert markedsføring. For at et forbud skal være rimelig, og også mulig å etterleve og håndheve, er det avgjørende at et forbud er klart definert. Et forslag om et generelt forbud mot atferdsbasert annonsering innebærer etter Moen og Næss sitt syn en forenkling. Det er avgjørende å regulere det som reelt sett er den største personvernrisikoen; datainnsamling på tvers av internett på en måte som er helt ugjennomsiktig og ukontrollerbar for brukerne.

Det er åpenbart ikke i forbrukernes interesse at nyhetsmediene svekkes. Moen og Næss mener at et eventuelt forbud mot atferdsbasert annonsering heller ikke er i forbrukernes interesse om man ser bort fra dette. I dag kan man knapt tenke seg et internett uten sorteringsmekanismer. Den grenseløse mengden informasjon som internett gir tilgang til blir ikke nyttig om den ikke kan sorteres og prioriteres. Dette er noe av kjernen i alle de fordelene internett og de sosiale nettverkene gir.

Moen og Næss støtter i likhet med flertallet et forbud mot bruk av data om barn og særlige kategorier data. I tillegg mener Moen og Næss at innsamling og bruk av data for å bygge og berike profiler på tvers av ulike behandlingsansvarlige er vanskelig for forbrukere å forstå og kontrollere. Et forbud mot slik bruk av tredjepartsdata bør utredes.

9.4.3 Manipulerende design

Manipulerende design er et samlebegrep om brukerdesign og grensesnitt som er laget for å lede forbrukerne til å ta valg som er i tjenesteleverandørens interesse, ofte på bekostning av forbrukerens egne interesser.[65] Det innebærer for eksempel at det som regel er mye lettere å tegne et abonnement enn å si det opp, eller at man blir lurt til å gi fra seg personopplysninger gjennom tungvinte eller forvirrende personverninnstillinger.[66] En studie gjennomført på vegne av Europakommisjonen i 2022, fant at 97 prosent av de 75 mest populære nettsidene og appene i Europa anvendte en eller flere typer manipulerende design. I en rapport skrevet av Forbrukerrådet fremkommer det at de globale teknologiselskapene dytter forbrukerne mot deling av personopplysninger gjennom bruk av «standardinnstillinger, utspekulerte designgrep, forvirrende oppsett og liksom-valg».[67, 68]

Standardinnstillinger er et kraftig verktøy for å få brukerne til å ta bestemte valg. Dersom standardinnstillingen er satt til å dele mest mulig personopplysninger, er mange forbrukere tilbøyelige til å la innstillingene være i fred, selv om det kan påvirke deres personvern negativt. I 2018 klaget Forbrukerrådet inn Alphabet (Google) til Datatilsynet for brudd på personvernforordningen på grunn av hvordan personverninnstillingene for lokasjonssporing var designet. Ifølge Forbrukerrådet hadde Alphabet designet disse innstillingene på en bevisst villedende måte, som var egnet til å få forbrukerne til å dele mest mulig opplysninger med selskapet.[69]

Bruken av manipulerende design er særlig problematisk i et personvernperspektiv fordi det undergraver samtykkekravet i personvernregelverket. Dersom tjenesteleverandører kan utforme samtykkemekanismer slik at forbrukere villedes til å samtykke til noe de ellers ikke ville samtykket til, kan man ikke snakke om et reelt og lovlig samtykke.

Det finnes regler mot villedende markedsføring i markedsføringsloven, og det er til dels overlappende krav til åpenhet og transparens i forbru-

---

65 Begrepet «dark patterns», et annet ord for manipulerende design, ble først introdusert av Harry Brignull i 2010, på nettsiden darkpatterns.org. hvor han beskrev brukerdesignet som «tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something.» Brignull, H. (u.å.). *What is deceptive design?*

66 Arunesh Mathur, A., Mayer, J. & Kshirsagar, M. (2021). What Makes a Dark Pattern…Dark?: Design Attributes, Normative Considerations, and Measurement Methods. *CHI Conference on Human Factors in Computing Systems (CHI '21)*.

67 Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., et al. (2022). *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation: final report.* Europakommisjonen.

68 Forbrukerrådet. (2018). *Deceived by design*.

69 Forbrukerrådet. (2018). *Every Step You Take.*

Boks 9.3 DULTING

Manipulerende design er en avart av fenomenet «dulting» (nudge). Dulting brukes gjerne for å beskrive grep som skal påvirke og endre atferd i positiv retning. For eksempel kan myndighetene påvirke forbrukernes atferd i positiv retning. Finanstilsynets innføring av regulering for kredittkortfaktura fra 2017 er et slikt tilfelle. For å avhjelpe den økende kredittkortgjelden i Norge, innførte Finanstilsynet i 2017 en forskrift som påla alle banker å utstede kredittkortfaktura med fullt, utestående beløp som standardalternativ. Dette var en endring fra tidligere, hvor bankene førte opp minstebeløpet som standard betalingsalternativ. Forskriften er en del av regjeringens arbeid med å forebygge gjeldsproblemer i private husholdninger.

I en masteroppgave fra NHH ble det undersøkt hvilken effekt endringen av standardalternativet har hatt på nedbetaling av kredittkortgjeld.[1] Funn fra oppgaven tyder på at endringen i beløpet på fakturaen påvirket forbrukerne som skyldte mest til å betale mer av kredittkortgjelden sin. Forfatterne av oppgaven registrerte den kraftigste effekten for kundene som i utgangspunktet betalte nær minimumsbeløpet.

Myndighetene dultet eller dyttet på denne måten forbrukerne til å gjøre noe som var bra – både for forbrukerne selv og for samfunnet som helhet. Eksempelet viser at standardalternativ kan være et mektig og kostnadseffektivt verktøy som kan brukes for å påvirke forbrukeratferd i ønsket retning.

1 Svardahl, A. & Aalen, H.K. (2020). *Can default options lead to credit card default? An empirical analysis of the effect of altered default options on credit card repaybehavior in Norway.* Masteroppgave. Norges Handelshøyskole.

kerlovgivningen og personvernregelverket med hensyn til hvordan forbrukerne skal informeres.[70] Samtidig er det vanskelige grensedragninger mellom hva som er manipulerende, villedende, eller overtalende design og språkbruk, og hva som ikke er det. Det kan være forskjellige forventninger fra forbrukers side om hva som er ønsket eller uønsket bruk av personopplysninger, noe som også kompliserer bildet. I Nederland har det nasjonale forbruker- og konkurransetilsynet publisert en veileder for digitale tjenesteleverandører, som har til hensikt å tydeliggjøre disse grensedragningene.[71]

Europaparlamentet har uttrykt et ønske om å forby bruken av manipulerende design i sin forhandlingsposisjon til den kommende forordningen om digitale tjenester (DSA).[72]

Personvernkommisjonen mener et forbud mot manipulerende design, som foreslått i DSA, vil styrke forbrukeres muligheter til å ivareta eget personvern på nett. Et slikt forbud bør kompletteres med håndheving av gjeldende forbrukerregelverk, samt med veiledere fra tilsynsmyndighetene som tydeliggjør grensedragningen mellom hva som vurderes som henholdsvis akseptabel og uakseptabel bruk av design. Et slikt forslag bør forankres og sikres gjennom EU-samarbeidet.

9.4.4 Informasjonsasymmetri

Behandling av personopplysninger innebærer ofte både kompliserte juridiske vurderinger og avtaler, samt avansert teknologi og uoversiktlige aktørbilder. I mange tilfeller vet ikke forbrukerne at personopplysninger behandles, hvem som behandler opplysningene, eller hva konsekvensene av behandlingen kan være. I tilfeller hvor personopplysninger deles videre med tredjepartsaktører – som for eksempel datameglere – er mange forbrukere ikke en gang klar over at selskapene som mottar personopplysninger eksisterer. Dette utgjør en form for *informasjonsasymmetri*, hvor selskaper vet mye om den enkelte forbruker, mens forbrukerne vet lite om selskapene og hvordan personopplysningene deres brukes.[73]

I et forbrukerperspektiv er det et grunnleggende problem at forbrukerne ikke har tilstrekkelig informasjon til å bedømme kvaliteten på det produktet de ønsker å kjøpe. I en kjøp- og salg-

70 Forbrukertilsynet og Datatilsynet. (u.å.). *Digitale tjenester og forbrukeres personopplysninger.*

71 Authority for Consumers & Markets. (2020, 11. februar). *Consumer better protected against misleading practices online.*

72 EU-parlamentet. (2022, 20. januar). *Digital Services Act: regulating platforms for a safer online space for users.*

73 Begrepet informasjonsasymmetri er hentet fra økonomisk teori, og beskriver situasjoner hvor en av partene i en økonomisk transaksjon har tilgang på mer informasjon enn motparten.

situasjon er ofte tilgangen til informasjon skjevt fordelt – selgeren vet mer om pris og kvalitet enn forbrukeren har mulighet til å vite. Når det gjelder behandling av personopplysninger, betyr informasjonsasymmetrien at det ofte er umulig for forbrukerne å ta et informert valg. For eksempel vil ikke en forbruker være i stand til å gjøre en informert beslutning om å dele data dersom vedkommende ikke forstår hvordan personopplysningene anvendes.

Mangel på åpenhet og informasjon skaper også utfordringer knyttet til forbrukernes mulighet til å ta i bruk sine lovfestede rettigheter, særlig i møte med store internasjonale selskaper. Selskapene kan ha begrenset nasjonal tilstedeværelse, ingen direkte kontaktpunkter forbrukerne kan benytte seg av og det kan generelt være vanskelig å få selskapene i tale. Selskapenes internasjonale karakter kan også medføre at det er et begrenset nasjonalt handlingsrom til å ta tak i utfordringer rundt informasjonsasymmetri.

Personvernkommisjonen ser derfor at forebygging av problemstillinger knyttet til informasjonssymmetri forutsetter internasjonalt samarbeid, særlig gjennom europeiske institusjoner.

9.4.4.1 Personvernerklæringer har ofte liten praktisk verdi for forbrukerne

Tilstrekkelig og korrekt informasjon er grunnlaget for at forbrukeren kan ta opplyste valg og inngå avtaler. Når en virksomhet behandler personopplysninger, skal den gi informasjon til de berørte. Personvernregelverkets krav knyttet til informasjon og åpenhet er omtalt i kapittel 4. Selv om virksomheter er pliktig til gi informasjon, er det likevel ofte slik at informasjonen forbrukerne har krav på ikke er tilgjengelig, er umulig å forstå, eller gjemmes bort.

Virksomheter kan gi informasjon til de berørte i en personvernerklæring. Personvernregelverket inneholder krav om at informasjonen skal gis på en kortfattet, åpen, forståelig og lett tilgjengelig måte. Språket skal være klart og enkelt, særlig når informasjonen er spesifikt rettet mot barn.[74] Til tross for at det er satt tydelige krav til

Boks 9.4 Personvernparadokset

Selv om forbrukere oppgir at de er opptatt av eget personvern, har mange forbrukere en tendens til ikke å ta få grep for å beskytte seg selv. Dette kalles *personvernparadokset,* en teori som har vært brukt for å argumentere for at forbrukere verdsetter bruk av digitale tjenester over eget personvern. Personvernparadokset er omdiskutert som fenomen, og det er uenighet knyttet til hva skillet mellom forbrukernes oppfatninger og handlingsmønster faktisk betyr.[1]

En studie fra University of Pennsylvania fra 2015 fant at amerikanske forbrukere i stor grad følte at det var umulig å ivareta eget personvern, og derfor hadde gitt opp å ta grep.[2] Det samme gjelder i Norge. Datatilsynets personvernundersøkelse fra 2019 viste at selv om åtte av ti nordmenn oppga at de var svært eller ganske opptatt av personvern, opplever seks av ti å «føle seg maktesløse når det gjelder å ha kontroll over personopplysninger på internett».[3] Dette kan skyldes en rekke faktorer, inkludert mengden aktører som samler inn data, kompliserte teknologier og verdikjeder, samt en rekke atferdspsykologiske effekter som utnyttes for å legitimere datainnsamling.

Følelsen av å ikke ha mulighet til å beskytte eget personvern kan lede til *personvernkynisme*, eller digital resignasjon,[4] hvor forbrukerne resignerer fra å forsøke å kontrollere personvernet. Som nevnt ovenfor har forbrukere ofte ikke noe valg, og det er så godt som umulig å navigere den digitale forbrukerhverdagen uten å spores og profileres. Det kan altså være en feiltolkning å anta at bruk av tjenester som ikke respekterer personvernet er det samme som å akseptere personvernbrudd. Tjenestetilbydere som har et økonomisk insentiv til å samle inn mest mulig personopplysninger kan utnytte personvernkynisme i et forsøk på å legitimere forretningspraksis som strider med personvernet.[5]

1 Solove, D.J. (2021). The Myth of the Privacy Paradox. *The George Washington Law Review, 89*(1).

2 Turow, J., Hennessy, M. & Draper, D. (2015). *The Trade-off Fallacy: How Marketers are Misrepresen American Consumers and Opening Them Up to Explo.*

3 Datatilsynet. (2020). *Personvernundersøkelsen 2019/ 2020.*

4 Draper, N.D. & Turow, J. (2019). The corporate cultivation of digital resignation. *SAGE Journals.*

5 Lutz, C., Hoffmann & C.P., Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany, *SAGE Journals.*

hvordan informasjon til de berørte skal gis, er fremdeles forekomsten av lange, omstendelige og vanskelig tilgjengelige personvernerklæringer høy. Forbrukerrådet har kartlagt utfordringer knyttet til informasjon og transparens i samarbeid med forbrukerorganisasjoner i andre land.[75]

Dersom forbrukerne skal kunne nyttiggjøre seg av informasjonen og tilpasse sin atferd for å sikre eget personvern, er det avgjørende at virksomheter utarbeider gode og brukervennlige løsninger.

En rekke studier som har vært gjennomført viser at så godt som ingen forbrukere leser personvernerklæringer.[76, 77] En studie fra 2009 anslo at det ville tatt 244 timer i året å lese alle personvernerklæringer en gjennomsnittsforbruker møter i hverdagen – et tall som trolig har vokst kraftig siden studien ble gjennomført.[78] Slik mange personvernerklæringer er utformet i dag har de altså som regel liten eller ingen nytteverdi for forbrukere.

9.4.4.2 Vanskelig å benytte seg av rettigheter

Den utstrakte innsamlingen og delingen av personopplysninger skaper også utfordringer knyttet til forbrukernes utøvelse av sine grunnleggende rettigheter. Som beskrevet i kapittel 4, gir personvernregelverket de registrerte rettigheter knyttet til blant annet innsyn, retting og sletting av egne personopplysninger. Det blir i praksis umulig å utøve disse rettighetene dersom man ikke vet hvilke personopplysninger som samles inn, og spesielt dersom man ikke vet at aktørene som behandler opplysningene eksisterer. Slik fører informasjonsasymmetrien også til en betydelig mangel på kontroll over egne personopplysninger.

Selv om forbrukerne får tilstrekkelig og forståelig informasjon om hvordan personopplysningene behandles, vil ikke informasjonen nødvendigvis gi forbrukerne innsikt i hvilke konsekvenser innsamlingen og eventuelt viderebehandlingen av opplysningene vil ha for deres personvern. Det er for eksempel vanskelig for forbrukerne å overskue hvilke konsekvenser det har for deres personvern at personopplysningene deres deles med, og viderebehandles av, flere titalls tredjepartsselskaper når de besøker en nettside.

Enkelte tjenesteleverandører tilbyr tilgangs- og gjennomsiktighetsverktøy («transparency tools») hvor forbrukerne kan finne informasjon om databehandlingen, eller om hvorfor de blir vist en bestemt annonse. Slike verktøy kan være nyttige og bidra til å holde tjenesteleverandørene ansvarlige for behandlingen av personopplysninger.

Hvis slike verktøy skal ha reell nytteverdi, må imidlertid informasjonen som gis være korrekt, uttømmende, detaljert og kommunisert på en forståelig måte, samt kunne verifiseres av tredjeparter.[79] Verktøyene bør for eksempel ikke informere kun om hvilke personopplysninger som samles inn om forbrukerne, men også gi informasjon om hvordan opplysningene eventuelt sammenstilles, hvilke personopplysninger som utledes ved hjelp av analyseverktøy, samt hvordan opplysningene viderebehandles og hvilke konsekvenser dette kan ha. Et gjennomsiktighetsverktøy, som forklarer hvorfor en forbruker ser en bestemt annonse ved å gi generell informasjon (kjønn, aldersspenn), vil for eksempel være av begrenset verdi dersom de faktiske målrettingskriteriene er mer granulerte (nøyaktig lokasjon, nettleserhistorikk, utledet informasjon). Teknologi for å fremme personvern er drøftet i kapittel 11.

Personvernkommisjonen mener verktøy for å tilgjengeliggjøre informasjon om hvilke personopplysninger som samles inn og hva de brukes til er nyttige for forbrukerne, journalister, tilsyn og lignende, og kan bidra til å holde næringsdrivende ansvarlige ved å synliggjøre problematisk praksis. *Kommisjonen* understreker imidlertid at den omfattende kommersielle innsamlingen, behandlingen og delingen av personopplysninger som har blitt normalisert i den digitale forbrukerhverdagen ikke kan løses kun gjennom å gi forbrukerne mer informasjon.

9.4.5 Diskriminering og manipulering

Den utstrakte innsamlingen av personopplysninger bidrar blant annet til at forbrukerne plasseres i forskjellige kategorier og segmenter. Dette kan for eksempel være nyttig ved at lignende brukere

---

74 Se personvernforordningen artikkel 5, 13 og 14.

75 Appfail kampanje, se oppsummerte punkter i Meld. St. 25 (2018–2019) *Framtidas forbrukar – grøn, smart og digital.* Barne- og familiedepartementet, s. 47.

76 Kon, G. (2018). *Does anyone read privacy notices?* Linklaters.

77 Brooke Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar & M., Turner, E. (2019). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.* Pew Research Centre.

78 McDon A.M. & Cranor, L.F., (2021). The Cost of Reading Privacy olicies. *I/S: A journal of law and policy for the information society, 2021 (01).*

79 Andreou, A., Venkatadri, G., Goga, O., Gummadi, K.P., Loiseau, P., Mislove, A. (2018). Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations. *NDSS 2018 – Network and Distributed System Security Symposium*, 1-15.

får anbefalt samme innhold, som i en anbefalingsalgoritme hos en strømmetjeneste. Samtidig oppstår det en rekke utfordringer dersom personopplysninger brukes for å forskjellsbehandle forbrukerne.

9.4.5.1 Påvirkning av sårbare grupper

En rekke digitale rettighetsorganisasjoner har avdekket hvordan datameglere kategoriserer forbrukerne i tusenvis av ulike segmenter basert på informasjon utledet fra analyse av omfattende mengder med personopplysninger.[80] Mange av segmentene er gjenkjennelige fra tradisjonell markedsføring (for eksempel mann 50+, interessert i engelsk fotball), og er i utgangspunktet relativt uproblematiske. Muligheten til å utlede detaljert kunnskap om enkeltforbrukere basert på innsamlede personopplysninger, har imidlertid ført til at det lages svært finmaskede segmenter om forbrukerne, av og til også basert på særlige kategorier av opplysninger. Det lages for eksempel segmenter basert på opplysninger om sykdom, religion, livsendringer (for eksempel dødsfall i familien eller nybakt forelder), og mye mer.

En rekke eksempler fra andre land har vist hvordan innsamlede personopplysninger har blitt brukt til å nå sårbare grupper i samfunnet med mårettede budskap. For eksempel har selskaper i finanssektoren i USA og Australia møtt kritikk for å ha målrettet markedsføring for forbrukslån mot økonomisk sårbare forbrukere, noe som kan ha bidratt til å forverre den økonomiske situasjonen deres ytterligere.[81] I Storbritannia har det blitt avslørt hvordan nettkasinoer og bettingselskaper bruker personopplysninger for å nå ut til forbrukere med spilleproblemer.[82]

Denne formen for målretting brukes ikke bare av kommersielle aktører. Politiske partier er også flittige brukere av atferdsbasert markedsføring.

Annonsesystemet til Facebook er kritisert for at det tillater målretting av budskap mot sårbare grupper. Det mest kjente eksemplet på dette var den såkalte Cambridge Analytica-skandalen, hvor dataselskapet Cambridge Analytica høstet brukerdata fra Facebook for å målrette politiske budskap blant annet basert på personlige sårbarheter hos Facebooks brukere.[83] Facebook har også møtt kritikk for at anbefalingsalgoritmene på plattformen anbefalte og tilrettela for målretting av desinformasjon om vaksiner i forbindelse med covidpandemien.[84]

I mars 2022 annonserte Europakommisjonen at de vil foreta en gjennomgang av flere sentrale forbrukerverndirektiver. Den kommende gjennomgangen av forbrukervernregelverkene er en viktig mulighet for EU- og EØS-medlemslandene til å foreslå nye og effektive tiltak for å redusere dagens forbrukersårbarhet.

Personvernkommisjonen anbefaler at det stilles strenge informasjons- og åpenhetskrav til hvordan forbrukerne profileres og segmenteres ved målretting av annonser og politiske budskap. Det innebærer at næringsdrivende, organisasjoner og politiske partier er åpne om hvilke budskap de sender ut, og hvem de forsøker å nå med budskapene. Plattformer som tilrettelegger for segmentering og profilering av forbrukerne bør også tilby verktøy for å vise hvilke annonser som vises på

Boks 9.5 Sensitive personopplysninger deles for markedsføringsformål

Den britiske organisasjonen Privacy International har avdekket hvordan en rekke digitale tjenester deler og selger personopplysninger som avdekker intime sårbarheter og hemmeligheter. Organisasjonen har blant annet vist at en rekke nettsteder rettet mot personer med psykiske lidelser sender personopplysninger til kommersielle partnere for markedsføringsformål,[1] at flere menstruasjonsapper deler svært detaljert informasjon med Meta,[2] og at diettapper samler inn og deler helseopplysninger med tredjeparter.[3]

1 Privacy International. (2020, 6. februar). *Mental health websites don't have to sell your data. Most still do.*

2 Privacy International. (2019, 9, september). *No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data.*

3 Privacy International. (2021, 4. august). *An unhealthy diet of targeted ads: an investigation into how the diet industry exploits our data.*

80 Irish Council for Civil Liberties. (2020, 21. september). *Two years of DPC inaction on the ongoing RTB data breach: Irish people with AIDS profiled, and Polish elections influenced.*

81 Harrison, P. & Gray, C. (2010). The ethical and policy implications of profiling 'vulnerable' customers. *International Journal of Consumer Studies*, vol. 34(4), 437-442.

82 Christl. W./Cracked Labs. (2022). *Digital Profiling in the Online Gambling Industry.* Clean Up Gambling.

83 The Gurdian. (2018, 17. mars). *Revealed: 50 million Facebook profiles harvested for CamAnalytica in major data breach.*

84 The Markup. (2021, 20. mai). *Facebook Said It Would Stop Recommending Anti-Vaccine Groups. It Didn't.*

plattformen, og hvilke segmenter de bruker. Åpenhet er nødvendig for å avdekke urimelig eller skadelig påvirkning. Regjeringen bør arbeide for å få på plass slike krav gjennom EU.

9.4.5.2 Urettmessig forskjellsbehandling og diskriminering

Personopplysninger kan samles inn og brukes til å urettmessig forskjellsbehandle eller diskriminere enkeltpersoner eller grupper av mennesker. Personopplysninger kan sammenstilles for å lage forbrukersegmenter, for eksempel basert på økonomisk situasjon og betalingsevne. Aviser og rettighetsorganisasjoner har avdekket at informasjon om blant annet betalingsevne, brukes til å selge den samme tjenesten til ulik pris.[85] Dette kan føre til at forbrukere med dårlig råd får mulighet til å kjøpe produkter og tjenester til en rimeligere pris, men det kan også brukes til å skape et A og et B-lag av forbrukerne basert på differensierende faktorer forbrukerne ikke har innsyn i eller kjenner til.

Som beskrevet i kapittel 5, kan det være svært utfordrende å avdekke om systemer basert på maskinlæring har skjevheter som fører til diskriminering. Skjevhetene skyldes feilkilder, lite representativt utvalg av data, ukorrekte data eller feil i selve systemet, eller fordi systemet brukes feil. Dersom en forbruker plasseres i feil kategori som følge av skjevheter i systemet, kan dette medføre at vedkommende utelukkes fra tjenester de egentlig har rett på, for eksempel ved en kredittvurdering. Diskriminering kan også skje dersom maskinlæringssystemet er basert på feilaktig grunnlag eller trent opp på skjevt datagrunnlag.

Personvernkommisjonen anbefaler at virksomheter som bruker maskinlæringssystemer for å profilere og segmentere forbrukerne bør rapportere hvordan de motvirker diskriminerende effekter i systemene. Offentlige myndigheter bør stille krav om slik rapportering ved anskaffelser og bevilgning av midler. Regjeringen bør arbeide for at slike krav blir en del av den kommende forordningen for kunstig intelligens med vedlegg.

9.4.5.3 Oljefondet som investor i teknologigigantene

Den norske stat er en betydelig investor i samtlige av de største teknologiselskapene gjennom Oljefondet. Fondet har i 2022 en aksjeandel på 0.85 prosent i Alphabet, 1.01 prosent i Meta, 0.81 prosent i Amazon, 0.84 prosent i Apple, og 0.95 prosent i Microsoft.[86]

Som en del av sitt mål om god og samfunnsansvarlig selskapsstyring, har Oljefondet publisert en rekke forventningsdokumenter hvor det stilles forventningskrav for ansvarlig og etisk virksomhet i selskaper fondet investerer i. Det inkluderer forventninger til bærekraft og klima, antikorrupsjon og menneskerettigheter.[87] Så vidt *Personvernkommisjonen* er bekjent, inneholder ingen av dokumentene forventninger knyttet til digitale rettigheter, personvern eller algoritmisk diskriminering, på tross av de betydelige investeringene i teknologigigantene. Dette synes heller ikke å være evalueringskriterier i Etikkrådets vurderinger av investeringer.

Personvernkommisjonen anbefaler at det stilles krav til ivaretakelse av personvernet, i likhet med krav som stilles til ivaretakelse av andre grunnleggende menneskerettigheter, når Oljefondet investerer i teknologiselskaper. Oljefondets forventningsdokumenter bør inkludere klare krav som fremmer åpenhet, etterrettelighet og etterlevelse av personvernrettigheter. Dette vil kunne bidra til å gjøre manglende beskyttelse av personvern til en investeringsrisiko.

Personvernkommisjonen anbefaler at Oljefondet avstår fra å investere i selskaper som krenker personvernet, og som det ikke har mulighet til å påvirke, for eksempel på grunn av majoritetseiere.

9.4.6 Svikt i markedet

Digitaliseringen av forbrukertjenester, der personopplysninger inngår som en sentral råvare, har ført til at det i dag er er viktig å se konkurranse-, forbruker- og personvernlovgivningen i sammenheng. Dette er avgjørende for å kunne ivareta forbrukernes rettigheter på en effektiv og helhetlig måte.[88]

I tradisjonelle, velfungerende markeder kan forbrukerne ofte bruke sin forbrukermakt til å påvirke næringsaktørers opptreden. Dersom man ikke er fornøyd med et produkt eller selskapets praksis, kan man gå til en konkurrent. Dette er

[85] CBC. (2017, 24. november). *How companies use personal data to charge different peodifferent prices for the same product.*

[86] Norges Bank Investment Management. (u.å.). *Investeringene.*

[87] Norges Bank Investment Management. (u.å.). *Ansvarlig forvaltning.*

[88] UK Competition and Markets Authority. (2021). *Algorithms: How they can reduce competition and harm consumers.*

ikke nødvendigvis overførbart til mange digitale forbrukermarkeder.

Brudd på personvernet skiller seg fra mer tradisjonelle skadevirkninger i at den som er rammet av bruddet ikke nødvendigvis er klar over at dette har skjedd. Det er for eksempel vanskelig for en kunde å avdekke at man har blitt utsatt for urettmessig forskjellsbehandling som følge av at gale opplysninger har blitt lagt til grunn og at man derfor har blitt plassert i en forbrukerkategori som hindrer en tilgang til en tjeneste man ellers hadde hatt krav på. Med jevne mellomrom dukker det opp personvernskandaler som får mye oppmerksomhet i media. Disse skandalene omfatter ofte tjenester forbrukerne er avhengige av (for eksempel Facebook), eller tredjepartstjenester som forbruker ikke har noe direkte forhold til. I førstnevnte tilfelle finnes det ofte ingen alternative tjenester å bytte til dersom forbrukeren er misfornøyd med hvordan selskapet ivaretar personvernet. I sistnevnte tilfelle finnes det ikke et kundeforhold de kan bryte. Dette kan betegnes som en markedssvikt – forbrukerne kan i mange tilfeller ikke bruke sin forbrukermakt til å «straffe» selskaper som ikke tar personvern på alvor.

9.4.6.1 De store teknologiselskapenes dominans

Dataøkonomien har bidratt til maktkonsentrasjon i flere digitale markeder. Noen få globale aktører har tilnærmet monopol på blant annet sosiale medier, søkemotorer og annonseplattformer. Dette er utfordrende for konkurransesituasjonen. Manglende konkurranse kan føre til høyere priser, mindre innovasjon og dårligere kvalitet for forbrukerne. I den digitale hverdagen vil dette ofte føre til dårligere personvern, fordi de største aktørene ikke trenger å konkurrere om å ivareta personvernet.

De største teknologiselskapene har opparbeidet seg dominerende markedsposisjoner blant annet gjennom akkumulering av data. Datainnsamlingen har bidratt til utvikling og forbedring av tjenester. Dette har skapt en selvforsterkende effekt der de største stadig blir større. Samtidig har teknologigigantene i mange tilfeller kjøpt opp konkurrerende tjenester, eller populære tjenester i tilgrensende markeder. Oppkjøp av tjenester fører til økt tilstrømning av brukere, og med dette økt tilgang til personopplysninger.

Når noen få enkeltselskaper får en dominerende stilling i viktige segmenter, kan disse selskapene også sette premisser for eventuelle konkurrenter. For eksempel bestemmer Alphabet og Apple vilkårene for hvilke aktører som får tilgang til app-butikkene deres. Dette kan medføre en viss kvalitetskontroll, men gir også selskapene stor makt, da de opptrer som portvoktere til viktige markedsplasser og bestemmer hvem som får slippe til.

De store plattformselskapene setter også premissene for hvordan personvernet ivaretas på plattformene sine, ved at de bestemmer hvilke

Boks 9.6 Selskapssammenslåing og kombinerte data

Da Alphabet (Google) kjøpte annonseteknologitjenesten DoubleClick i 2007, var det under premiss om at data fra DoubleClick ikke skulle kombineres med brukerdata fra Googles andre tjenester. I 2016 gikk selskapet tilbake på lovnaden, og slo sammen informasjonen.[1] I 2019 påla tyske forbrukermyndigheter Meta (Facebook) å ikke lenger kombinere brukerdata på tvers av tjenester som Facebook, WhatsApp og Instagram. Myndighetene begrunnet vedtaket med at Facebooks sammenslåing av brukerdata var misbruk av selskapets dominerende markedsposisjon, samt at personvernkonsekvensene ved sammenslåingen var til skade for forbrukerne.[2]

Konkurransemyndigheter rundt om i Europa har også fusjonskontrollverktøy for å stoppe oppkjøp som har konkurransehemmende effekt. I løpet av de siste årene har blant annet britiske konkurransemyndigheter utstedt en ordre mot Metas oppkjøp av tjenesten Giphy,[3] mens Europakommisjonen påla Alphabet en rekke begrensninger på bruk av personopplysninger ved oppkjøp av selskapet FitBit.[4]

1 ProPublica. (2016, 21. oktober). *Google Has Quietly Dropped Ban on Personally IdentifiWeb Tracking.*

2 Bundeskartellamt. (2019, 7. februar). *Bundeskartellamt prohibits Facebook from combining user data from different sources.*

3 UK Competition and Markets Authority. (2021, 30. november). *CMA directs Facebook to sell Giphy.*

4 Europakommisjonen. (2020, 17. desember). *Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions.*

muligheter tredjeparter har til å samle inn personopplysninger, og hvordan forbrukere eventuelt kan begrense innsamlingen. Det kan være et demokratisk problem at et knippe store globale selskaper har fått denne typen definisjonsmakt over ivaretakelsen av forbrukernes personvern.

Den utstrakte innsamlingen og analysen av personopplysninger kan også føre til høyere priser og dårligere utvalg av produkter. Et eksempel er Amazon – et av plattformselskapene som også produserer egne produkter, og selger dem på plattformen sin i konkurranse med tredjepartsselgere. Amazon bruker opplysninger om sine brukere – både næringsdrivende og forbrukere – til å identifisere produktgrupper av høy interesse. Denne innsikten bruker selskapet videre til å bestemme hvilke egenproduserte produkter de bør satse på. På bakgrunn av dette, har plattformgiganten høstet kritikk for å misbruke markedsmakten sin for å oppnå urimelige konkurransefordeler ved å prise ut konkurrentene på sin egen plattform.[89]

Alphabet har blitt bøtelagt av Europakommisjonen for å ha anbefalt forbrukerne sin egen handelsplattform på bekostning av konkurrentenes plattformer. Dette har vært mulig fordi Alphabet eier verdens største søkemotor.[90] Slik dataøkonomien fungerer i dag kan den føre til svekket innovasjon og økte priser ved å gjøre det vanskelig for andre, og nye, aktører å slippe inn på markedet.

De største plattformene karakteriseres også av å eie flere tjenester på tvers av markeder. Amazon er for eksempel en stor aktør på blant annet netthandel, strømmetjenester, skytjenester og infrastruktur. Dersom en plattform allerede har et stort antall brukere, kan dette senke etableringskostnadene i nye markeder betraktelig. Det kan skape utfordringer for norske aktører dersom globale plattformer inntar det norske markedet, og bruker sin eksisterende brukermasse til å overta store deler av kundegrunnlaget.

I 2019 trådte det reviderte betalingstjenestedirektivet (PSD 2) i kraft i Norge. Dette direktivet endret blant annet definisjonen av betalingstjeneste til å også inkludere andre aktører enn banker.[91] Det er forespeilet at PSD 2 vil utvide markedet for betalingstjenester, og at teknologigigantene vil lansere egne betalingstjenester for å konkurrere med bankene. Datatilsynets personvernundersøkelse 2019/2020 viste imidlertid at norske forbrukere i stor grad mener det er problematisk for personvernet sitt å gi Alphabet og Meta tilgang på sine finansielle opplysninger i banken for å tilby nyttige banktjenester.[92]

Som beskrevet i avsnitt 9.3.2, arbeides det i EU for å få på plass nye regler for å begrense maktkonsentrasjonen i det digitale tjenestemarkedet. De største teknologiselskapene, eller portvokterne, vil måtte forholde seg til strengere krav i den kommende forordningen om digitale markeder (DMA).[93] Rettsakten vil lovfeste forbud mot en rekke konkurransehemmende aktiviteter. Dette

Boks 9.7 Nettverkseffekter

En av årsakene til svak konkurranse mellom mange digitale tjenester skyldes omfattende *nettverkseffekter*. Nettverkseffekter gjør det mulig for store selskaper å bli så store at de til slutt dominerer markedet.

Nettverkseksternaliteter, også kalt nettverkseffekter, oppstår når hver ny bruker av en vare eller tjeneste skaper verdi for eksisterende brukere av varen eller tjenesten. Disse nettverkseffektene skaper en positiv forsterkende spiral ved at antall forbindelser mellom deltakerne i nettverket vokser mye raskere enn antall deltakere. De som lykkes best kan her ende opp med hva man kan kalle naturlige monopoler. Facebook er et eksempel på dette.

Dess større disse plattformene er, jo flere bedriftskunder får de også. Dette fører til en snøballeffekt, hvor de største aktørene har gode forutsetninger for å samle inn stadig flere opplysninger, som de kan anvende til å videreutvikle tjenester som er vanskelig for mindre aktører å konkurrere med.[1]

[1] Slettemeås, D. (2018). *Kunnskapsoppsummeringer til stortingsmelding om forbrukerpolitikk 2018. Forbrukernes digitale hverdag – utvidet versjon.* Forbruksforskningsinstituttet SIFO. OsloMet.

[89] BusinessInsider. (2020, 11. november). *Amazon, Google, and Alibaba face anticompetitive investifrom governments in the EU, China, and India.*

[90] Techcrunch. (2017, 27. juni). *Google sued in Europe for $2.4BN in damages over Shopantitrust case.*

[91] Europaparlaments- og Rådsdirektiv (EU) 2015/2366 om betalingstjenester i det indre marked om endring av direktiv 2002/65/EF, 2013/36/EU og 2009/110/EF og opphéving av direktiv 2007/64/EF (PSD 2)

[92] Datatilsynet. (2020). *Personvernundersøkelsen 2019/2020.*

[93] Forslag til europaparlaments- og rådsforordning om åpne og rettferdige markeder i den digitale sektoren (DMA) (2020).

inkluderer krav om å la forbrukere bytte eller melde seg ut av tjenester, samt et forbud mot å kombinere brukerdata på tvers av tjenester. Det er forespeilet at Europakommisjonen vil etablere en egen intern enhet som kan føre tilsyn med portvokterne, eller bidra i nasjonale tilsynssaker.

Personvernkommisjonen anbefaler at Norge tar initiativ til, og leder, et internasjonalt arbeid for å utrede hvordan virkemidler i konkurranseloven kan anvendes for å forhindre negative personvernkonsekvenser ved oppkjøp og fusjoner. Utredningen må vurdere om konkurranseloven er innrettet slik at den kan håndtere utfordringene i dataøkonomien på en effektiv måte. Dette må også sees i forbindelse med innføringen av nye konkurranseverktøy under den kommende forordningen om digitale markeder (DMA).

9.4.6.2 Innelåsning

Mange digitale tjenester er preget av problematiske *innelåsingseffekter* som gjør det vanskelig for forbrukerne å utøve forbrukermakt ved å bytte tjenester. Slike mekanismer kan være både tekniske, praktiske, økonomiske, eller de kan inngå i avtalevilkår. Tekniske innelåsingsmekanismer kan for eksempel være at man ikke har mulighet til å bruke tilkoblede produkter fra forskjellige leverandører sammen. Dette fører til at man føler seg låst til å fortsette å kjøpe produkter fra samme produsent.

Eksempler på innelåsende vilkår er lange bindingstider og høye gebyrer for å avslutte abonnementer, lange oppsigelsestider eller krav om at oppsigelse må skje på visse måter. Det kan også innebære bruk av manipulerende design som gjør det vanskelig å finne ut hvordan man sier opp en tjeneste.[94] Tjenesteleverandører har gjerne et økonomisk insentiv til å låse inn forbrukerne. Det er fordi dette både bidrar til at kunder blir værende, og at det kan føre til mersalg dersom man er låst inne i leverandørens økosystem.

Eksempelvis kan man forestille seg at en ny aktør bestemmer seg for å lansere et alternativ til Facebook, med en uttalt målsetning om å samle inn minst mulig personopplysninger, samtidig som tjenesten tilrettelegger for deling av innhold og sosial kontakt på en måte som minner om Facebooks tjenester. Nettverkseffekter (se beskrivelse i faktaboks) fører til svært høye oppstartskostnader, fordi de færreste ønsker å være på et sosialt medium med nesten ingen andre brukere. Dersom det ikke er på plass tekniske løsninger for å kommunisere med brukere utenfor plattformen, eller flytte innholdet sitt over til konkurrenten, blir forbrukerne i praksis innelåst. Byttekostnaden blir for høy for de fleste forbrukere.

Innelåsingseffekter kan forsterkes ved at forbrukerne blir vant til å bruke bestemte grensesnitt. Dette fører til at byttekostnadene blir høye fordi man må lære seg et nytt system dersom man bytter leverandør. For eksempel kan bruken av enkelte tjenesteleverandører i skolen føre til at elever blir låst til disse leverandørene senere i livet. Tjenesteleverandører kan dermed oppnå langsiktige kundeforhold ved å levere tjenester til skolevesenet, som diskutert i kapittel 8.

9.4.6.3 Manglende teknisk interoperabilitet og dataportabilitet

Innelåsing og problematiske nettverkseffekter kan blant annet imøtegås ved å implementere løsninger og standarder for teknisk interoperabilitet og dataportabilitet.[95] Teknisk interoperabilitet betyr at tjenester kan «snakke sammen» på tvers, uavhengig av hvilken tjenesteleverandør man bruker. For eksempel kan Telenorkunder ringe og sende meldinger til Teliakunder fordi telenettverkene er interoperatible. Dette er i liten grad tilfelle i digitale forbrukertjenester. Dersom man vil sende meldinger til noen som bruker Facebook Messenger må man selv også ha en Facebookprofil. Det er ikke mulig å bruke en konkurrerende tjeneste uten at vedkommende man vil sende en melding til også bytter tjeneste. Dette fører til byttekostnader som kan hemme konkurransen, og gjør det vanskeligere for personvernvennlige utfordrertjenester å entre markedet.

Mangel på portabilitet kan også bidra til uforholdsmessige store byttekostnader. I telekomsektoren i Norge har man nummerportabilitet. Det innebærer at kunder kan beholde telefonnummeret sitt dersom de bytter leverandør. Dersom man som kunde måtte bytte telefonnummer ved bytte av leverandør, ville byttekostnadene ved å tegne nytt abonnement vært uforholdsmessig høye.

Retten til dataportabilitet er hjemlet i personvernforordningen artikkel 20. Rettigheten innebærer at den registrerte kan kreve å få utlevert opplysninger om seg selv i et strukturert, vanlig og maskinlesbart format. Formålet er at den registrerte skal kunne ha mulighet til å flytte personopplysningene sine til andre tilbydere. Det er i

[94] Forbrukerrådet. (2021, 14, januar). *Amazon vil ikke gi slipp på kundene.*

[95] Privacy International. (2020, 20. august). *Explainer: Competition, Data and Interoperability in digimarkets.*

Boks 9.8 Teknisk interoperabilitet og portabilitet

Teknisk interoperabilitet betyr at forskjellige tjenester kan «snakke sammen». For eksempel kan man overføre penger på tvers av forskjellige banker fordi tjenestene er interoperatible. Dataportabilitet betyr at man kan flytte data mellom forskjellige tjenesteløsninger. For eksempel kan det innebære at man kan flytte data mellom forskjellige skytjenester.

Samlet sett bidrar teknisk interoperabilitet og dataportabilitet til at det er lettere å bytte mellom tjenesteleverandører.

hovedsak opplysninger som forbrukeren selv har gitt til den behandlingsansvarlige som er omfattet av retten til dataportabilitet.

Dataportabilitet skal i utgangspunktet bidra til at den registrerte får mer kontroll over personopplysningene sine.

For å være en praktisk anvendelig rettighet er det imidlertid viktig at dataportabilitet kombineres med teknisk interoperabilitet. Det har lite nytteverdi å kunne flytte e-postene sine ut av en e-posttjeneste dersom man ikke kan importere disse til en annen e-posttjeneste. Derfor er det avgjørende at det finnes felles tekniske standarder som bidrar til interoperabilitet. Forordningen om digitale markeder (DMA) vil stille krav til portvoktere om å tilby verktøy for å tilrettelegge for slik interoperabilitet.[96]

Den digitale forbrukerhverdagen kunne sett svært annerledes ut dersom flere tjenesteleverandører praktiserte portabilitet og teknisk interoperabilitet. Dersom man kunne kommunisere med hverandre på tvers av meldingstjenester, ville byttekostnaden vært lav nok til at forbrukere som er opptatt av personvern ville kunne velge et personvernvennlig alternativ, uten å måtte overbevise venner og familie om å bytte. Det ville bidratt til at personvern ble en konkurransefaktor, ved at misfornøyde forbrukere kunne bytte leverandør uten å gi avkall på nødvendige tjenester. Dermed ville nettverkseffektene svekkes i personvernets favør.

Personvernkommisjonen mener offentlige myndigheter bør stimulere til utvikling av løsninger og standarder for dataportabilitet og teknisk interoperabilitet. Forekomsten av slike løsninger er en forutsetning for sunn konkurranse i mange digitale vare- og tjenestemarkeder.

9.4.6.4 Personvern ikke en konkurransefordel

Norske myndigheter har i flere stortingsmeldinger og strategier uttrykt at personvern bør være en konkurransefordel. Dersom tjenestetilbydere anser det som et konkurransefortrinn å utvikle personvernvennlige løsninger, vil det stimulere til innovasjon i personvernets favør. Imidlertid kan personvern i mange tilfeller oppleves som konkurransehemmende. Aktører som samler inn og behandler personopplysninger i utstrakt grad – uten å sørge for et godt personvern – kan oppnå konkurransefordeler ved å ha tilgang på større mengder data enn sine konkurrenter, samt ved å unngå kostnader forbundet med å etablere personvernrutiner og lignende.

For eksempel samler norske medievirksomheter som regel kun inn opplysninger om brukerne på sine egne digitale flater. Store globale plattformaktører, som Google og Facebook, samler inn personopplysninger fra en lang rekke forskjellige nettsteder som har implementert sporingsteknologi fra selskapene. Opplysningene som samles inn, kan gi unike innsikter som benyttes til markedsføring. Slik har de store aktørene overtatt stadig større andeler av annonsemarkedet.

Mangelen på like spilleregler innenfor utvikling og bruk av forbrukertjenester er en grunnleggende utfordring for personvernvennlige og personvernfremmende forbrukertjenester. Som beskrevet i kapittel 13, har håndhevingen av regelverket overfor teknologigigantene så langt ikke vært tilstrekkelig effektiv. Dersom personvernregelverket ikke håndheves effektivt og strengt overfor grove overtredelser, medfører det lav risiko for teknologigantene i å ikke ivareta grunnleggende personvernprinsipper. En slik situasjon kan bidra til et kappløp mot bunnen, der de lovlydige taper terreng mens de som ikke etterlever regelverket kaprer stadig større markedsandeler. Mangelfull håndheving kan også føre til at det i praksis ikke oppleves som lønnsomt å innovere innenfor teknologi som ivaretar forbrukernes rettigheter.

Personvernkommisjonen mener det er en grunnleggende forutsetning for godt personvern at det skal straffe seg å bryte loven. Effektiv håndhevelse av personvernregelverket er derfor nødvendig for å etablere like spilleregler, og for å stimulere til innovasjon innenfor personvernfremmende teknologi.

[96] Digital Markets Act art. 6 nr. 1 bokstav h.

Personvernkommisjonen mener det er problematisk for personvernet at norske selskaper og globale teknologigiganter ikke opererer under like konkurransevilkår. Regjeringen må ta grep for å begrense gigantenes markedsmakt for å sikre like spilleregler, og slik tilrettelegge for innovasjon som støtter opp under personvernet.

9.5 Barn som forbrukere

Personvernkommisjonens mandat inkluderer å foreslå tiltak som styrker den digitale forbrukerkompetansen til barn og unge, spesielt knyttet til digital innsamling av personopplysninger og markedsføring i sosiale medier. *Kommisjonen* skal se på hvordan bruk av sosiale medier påvirker personvernet og kartlegge personvernkonsekvenser ved profilering av barn og direkte markedsføring, samt utrede barns samtykkekompetanse. *Personvernkommisjonen* vil derfor i denne delen av utredningen vektlegge hvilke utfordringer digitale tjenester kan skape for barns personvern. Som en del av denne drøftelsen vil *kommisjonen* også se på personvernutfordringer for barn i en familiekontekst.

Den digitale utviklingen har mange positive følger for barn og unge, som også tas i betraktning når *kommisjonen* ser på det totale bildet. Digitaliseringen har tilrettelagt for tilgang til informasjon, sosialt samvær, underholdning og læring for barn og unge. Den bidrar til å forsterke rettigheter som retten til ytringsfrihet og til informasjon. Disse rettighetene må sees i sammenheng med retten til personvern. Det må være en forutsetning at tjenesteleverandører som har barn og unge blant sine brukere, ivaretar barns grunnleggende rettigheter, og ikke setter rettighetene opp mot hverandre dersom det kan unngås.

Barn er i mange tilfeller mer sårbare enn voksne på grunn av manglende erfaring, økt impulsivitet, og lavere nivå av konsekvenstenkning. Selv om barn og unge i dag kan ha høy digital kompetanse, innebærer ikke dette nødvendigvis kunnskap om hvordan personopplysninger behandles, eller hvorfor personvern er viktig. Dette bidrar til at maktasymmetrien som beskrives i avsnitt 9.4. blir større i situasjoner som involverer barn.

9.5.1 Barns forbrukerhverdag

Barn og unge er ivrige brukere av digitale tjenester, både på skolen og i barnehagen, som beskrevet i kapittel 8, og på fritiden. Mange barn bruker sosiale medier for å holde kontakt med venner, nettaviser og videotjenester for å oppsøke informasjon, spill for å underholdes, og mye mer. Selv om barn og unge i mange tilfeller bruker andre nettsider og applikasjoner enn voksne, er typen digitale tjenester de bruker altså relativt lik. Barn og unge forholder seg likevel annerledes til mange av tjenestene de bruker enn det voksne gjør.

Gjennom digital teknologi kan barn få realisert sine sivile, politiske, kulturelle og sosiale rettigheter. Ulik tilgang på teknologi kan imidlertid føre til forskjeller mellom barn innad i et land og land imellom når det kommer til i hvilken grad de får realisert rettighetene sine ved bruk av teknologi.

Barn og unge er selvsagt ikke en homogen gruppe, og den digitale forbrukerhverdagen til en 17-åring skiller seg betraktelig fra en treårings. Den digitale forbrukerkompetansen varierer tilsvarende, og kan også henge sammen med andre faktorer, inkludert økonomisk situasjon og foreldres kompetanse. Det er relevant å nevne at mange av dagens småbarnsforeldre selv har vokst opp med internett, sosiale medier og smarttelefoner. Dette utgjør et skille fra tidligere foreldregenerasjoner, som ofte kunne sies å ha lavere digital kompetanse enn barna. Dermed er det i dag ikke nødvendigvis slik at foreldrene mangler grunnleggende digital kompetanse sammenlignet med barna.

Medietilsynets undersøkelse fra 2020 viser at 97 prosent av 9 til 18-åringer i Norge har egen mobiltelefon og at nesten halvparten av norske barn i alderen 1 til 5 år har tilgang til nettbrett.[97] Syv av ti barn ser på YouTube/YouTube Kids, mens litt over halvparten spiller digitale spill. I aldersgruppen 9 til 18 år bruker ni av ti sosiale medier. De mest populære plattformene i denne aldersgruppen er YouTube, SnapChat, TikTok og Instagram.[98] Det betyr at barn og unge er til stede på plattformer som samler inn store mengder personopplysninger for markedsføringsformål og andre formål.

9.5.2 Barns rettigheter i digitale flater

Selv om barn og unge i mange tilfeller har relativt høy digital kompetanse, vil de i mange sammenhenger være særlig sårbare. På grunn av denne underliggende sårbarheten har barn særskilt krav på beskyttelse, og flere relevante lovverk har særbestemmelser for barn og unge. Nedenfor gjøres det rede for de mest relevante lovene og rettighe-

[97] Medietilsynet. (2020.) *Småbarn og medier 2020.*
[98] Medietilsynet. (2020). *Barn og medier 2020.*

tene som har særlig betydning for barn og unges personvern.

9.5.2.1 Barns forbrukerrettigheter

Markedsføring overfor forbrukerne reguleres av EU-direktiv om urimelig handelspraksis[99] og markedsføringsloven.[100] EU-direktivet forbyr «urimelig handelspraksis» overfor forbrukerne.[101] Det er fremhevet at det alltid vil ansees urimelig og forbudt å inkludere «direkte oppfordringer til barn om å kjøpe annonserte produkter eller overtale foreldrene eller andre voksne til å kjøpe de annonserte produktene til dem» i reklame for barn.[102]

Markedsføringsloven har et eget kapittel som omhandler markedsføring rettet mot barn.[103] Som hovedregel skal virksomhetene vise «særlig aktsomhet overfor barns påvirkelighet, manglende erfaring og naturlige godtroenhet.» Videre skal det tas «hensyn til alder, utvikling og andre forhold som gjør barn spesielt sårbare».[104] Det foreligger et generelt forbud mot «urimelig handelspraksis».

I vurderingen må virksomhetene legge vekt på om markedsføringen er særskilt rettet mot barn.[105] Videre skal det legges vekt på om markedsføringen, «på grunn av art eller produkt, er egnet til å påvirke barn, og om den næringsdrivende kan forventes å forutse barns særlige sårbarhet for praksisen». Dette skal gjøres selv om markedsføringen ikke er særskilt rettet mot barn.[106] Til slutt skal markedsføringen ikke stride mot god markedsføringsskikk.[107] Forbrukertilsynet fremhever at det ved den generelle vurderingen skal «legges vekt på om markedsføringen krenker alminnelige etikk- og moraloppfatninger, eller om det tas i bruk støtende virkemidler».[108]

Selv om reglene er skjønnsmessig utformet, er prinsippene relativt klare. Virksomheter skal ta hensyn til barn når de er, eller kan være i, gruppen markedsføringen når ut til.

Boks 9.9 FNs barnekomité om barns rettigheter i digitale miljøer

FNs barnekomité har kommet med en generell kommentar som omtaler barns rettigheter i tilknytning til digitale miljøer.[1] Uttalelsene fra FNs barnekomité utgjør viktige holdepunkter og retningslinjer for norske myndigheters arbeid med å gjennomføre forpliktelsene etter konvensjonen.

Komiteen uttaler at statene bør gjøre barnets beste til det viktigste prinsipp når de regulerer reklame og markedsføring som er rettet mot og tilgjengelig for barn. Sponsing, produktplassering og alle andre former for kommersielt drevet innhold skal skille seg tydelig fra annet innhold og skal ikke videreføre kjønn- eller rasestereotypier.

Videre bør statene ifølge tolkningsuttalelsen i egne lovverk forby profilering av eller målretting mot barn i alle aldre for kommersielle formål på grunnlag av en digital registrering av deres faktiske eller avledede egenskaper. Teknologi som innebærer neuromarketing, emosjonell analyse, oppslukende reklame og reklame i virtuelle og utvidede virkelighetsmiljøer for å markedsføre produkter applikasjoner og tjenester, bør også forbys rettet direkte eller indirekte mot barn.

[1] Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, 2. march 2021.

Som beskrevet ovenfor, brukes personopplysninger til å utlede atferd, preferanser, evner eller behov. Denne kunnskapen brukes til å lage profiler og segmenter som brukes til å målrette markedsføring. Det kan argumenteres for at profilering for markedsføringsformål ikke er i henhold til god markedsføringsskikk. I sin markedsføringsveileder er Datatilsynet også klare på at virksomheter ikke skal profilere barn for markedsføringsformål.[109]

På tross av at bruk av atferdsbasert markedsføring mot barn som regel vil være forbudt, ser man gjentakende eksempler på markedsføring som klart er utenfor de lovlige rammene både

[99] Europaparlaments- og Rådsdirektiv 2005/29/EF av 11. mai 2005 (direktiv om urimelig handelspraksis).

[100] Lov om kontroll med markedsføring og avtalevilkår mv. (markedsføringsloven).

[101] Se direktiv om urimelig handelspraksis artikkel 5.

[102] Se direktiv om urimelig handelspraksis, vedlegg 1 punkt 28.

[103] Se markedsføringsloven kapittel 4.

[104] Se markedsføringsloven § 19.

[105] Se markedsføringsloven § 20.

[106] Se markedsføringsloven § 20 første ledd.

[107] Se markedsføringsloven § 21 og § 2.

[108] Forbrukertilsynet. (u.å.). *Forbrukertilsynets veiledning om handelspraksis overfor barn og unge.*

[109] Forbrukertilsynet og Datatilsynet. (u.å.). *Digitale tjenester og forbrukeres personopplysninger.*

direktivet for urimelig handelspraksis og markedsføringsloven setter opp.

Barneombudet og Forbrukerrådet har etterlyst en gjennomgang av markedsføringsregelverket for å se hvordan det kan innrettes for å beskytte barn bedre mot kommersiell utnyttelse på nett. De hevder at «forbrukerlovgivningen er fragmentert, uoversiktlig og med uklar ansvarsfordeling mellom tilsynsmyndighetene». For å oppdatere regelverket til å kunne beskytte barn og unge i digitale flater, foreslås det at regjeringen nedsetter et utvalg for å gjennomgå og foreslå endringer i de relevante regelverkene, inkludert bransjedrevne selvreguleringsordninger, og gjør en barnerettsvurdering av alle forslag som berører barn som forbrukere.[110]

Personvernkommisjonen anbefaler at Regjeringen nedsetter et lovutvalg for å gjennomgå og foreslå endringer i regelverk for å beskytte barn og unge i digitale flater.

9.5.2.2 Barneloven – Rekkevidde og begrensninger for foreldreansvaret

Barneloven regulerer foreldres rettigheter og plikter overfor barn, samt barns rettigheter overfor foreldre. De som har foreldreansvaret har rett og plikt til å bestemme for barna innenfor lovens grenser og barns med- og selvbestemmelsesrett, som omtales nærmere under. Barnelova § 30 regulerer innholdet i foreldreansvaret. Foreldreansvaret skal utøves ut fra barnets interesser og behov, jf. barnelova § 30 første ledd, fjerde punktum. Foreldrenes avgjørelser må også ta hensyn til barnets egne meninger og gradvise selvbestemmelsesrett, jf. barnelovens §§ 31 og 33.

Foreldres mulighet til å ivareta barns personvern er ikke direkte regulert i lovgivningen, men kan utledes av blant annet barnelova § 30.

I NOU 2020: 14 vises det til at enkelte utredninger peker på vergemålsloven som det rettslige rammeverket for spørsmålet om hvem som kan samtykke til behandling av personopplysninger på vegne av barn.[111]

Utgangspunktet etter barnelova er at alle beslutninger et barn ikke kan foreta på egenhånd, tilfaller foreldrene.[112] Imidlertid kan det i grensesnittet mellom barn og foreldre oppstå en rekke problemstillinger av interesse for barns kontroll over eget personvern. Barnelova supplerer de generelle personvernreglene når foreldre forvalter barnets rettigheter på vegne av barnet.

Personvernrettigheter kan utøves av foreldre alene, av barn og foreldre i samarbeid[113] eller av barnet alene. Når barnet er fylt 12 år, skal det legges stor vekt på hva barnet mener. Dette følger av barnelova § 31 andre avsnitt. Forslag til ny barnelov § 6-6, foreslår at denne aldersgrensen fjernes.

9.5.2.3 Foreldres bestemmelsesrett

Foreldrene har samtykkekompetanse på vegne av barnet på de fleste områder av barnets liv, med mindre det foreligger hjemmel for noe annet. Dette er særegent for forholdet mellom barn og foreldre, da det rettslige utgangspunktet er at den enkelte bare kan samtykke på vegne av seg selv. At bestemmelsesretten må utøves ut fra barnets interesser og behov, gjelder også samtykke og offentliggjøring etter personopplysningsloven, og samtykke til å offentliggjøre bilder og personopplysninger i media. Det følger derfor allerede av barneloven § 30 og foreldrenes omsorgsplikt at foreldrene ikke selv kan offentliggjøre eller samtykke i offentliggjøring av bilder og opplysninger om barna hvis dette ikke er til barnets beste. Også barnekonvensjonen artikkel 3 om barnets beste vil være til hinder for dette. Barnets rett til beskyttelse mot innblanding i privatlivet – barnets personvern – er imidlertid en tilstrekkelig begrunnelse i seg selv for å begrense foreldrenes samtykkekompetanse.

Foreldrenes bestemmelsesrett er også begrenset av flere regler. De mest sentrale begrensningene er barnets med- og selvbestemmelsesrett.

9.5.2.4 Barnets medbestemmelses- og selvbestemmelsesrett

Barns *medbestemmelsesrett* i alle spørsmål som angår dem, følger av barnekonvensjonen artikkel 12, grunnloven § 104, og av barneloven § 31, samt flere bestemmelser i særlovgivningen. Etter barneloven § 31, er dette en absolutt rett fra barnet er syv år når det gjelder saker om personlige forhold. Barn skal også høres før de har nådd denne

---

[110] Engh, I.B. (Barneombud) & Blyverket, I.L. (Forbrukerrådet). (2022, 30. januar). *Barneromsdøren står åpen for kommersielle aktører.* Dagens Næringsliv.

[111] I NOU 2020: 14 punkt. 8.5.7 vises det til bl.a. Prop. 56 LS (2017–2018), punkt 13.1, som igjen viser til forarbeidene til vergemålsloven som omtaler at den mindreårige ikke har kompetanse til å samtykke til behandling av egne personopplysninger. Smith 2011, mener at henvisningene til vergemålsloven på dette området er uriktige (Smith 2011, s. 115).

[112] Barnelova §§ 30, 31-33.

[113] Barnekonvensjonen art.12, jf. barnelova § 33.

alderen, hvis det dreier seg om saker hvor de har mulighet til å gjøre seg opp en mening. Barnets rett til å bli hørt vil i praksis si at barnets stemme bør bli utslagsgivende etter hvert som barnet blir eldre.[114]

Parallelt med medbestemmelsesretten, skal barn også ha en *selvbestemmelsesrett*, jf. barneloven § 33. Det følger av bestemmelsen at «foreldra skal gje barnet stendig større sjølvråderett med alderen og fram til det er myndig». Det avgjørende for når selvbestemmelsesretten inntrer er, på samme måte som ved medbestemmelsesretten, avhengig av hvilken type avgjørelse som skal tas, barnets alder og modenhet. Når barnet er modent nok til å treffe en forsvarlig avgjørelse, gjør begrunnelsen bak foreldreansvaret seg ikke lenger gjeldende, noe som taler for at barnet kan bestemme selv.[115]

9.5.2.5 Barns samtykkekompetanse

Full samtykkekompetanse til behandling av personopplysninger inntrer når en person fyller 18 år. Mindreårige har altså som hovedregel ikke slik kompetanse, jf. vergemålslova § 9. Et sentralt unntak er gjort ved barns bruk av informasjonssamfunnstjenester, jf. personvernforordningen artikkel 8 nr. 1, jf. personopplysningsloven § 5. Etter bestemmelsene har barn samtykkekompetanse fra de er 13 år ved det aller meste av sin internettaktivitet. Dette gjelder også der de benytter tjenester som ikke konkret er rettet mot barn, som ved bruk av sosiale medier. (Se nærmere om barnet som registrert person og barnets rettigheter etter personvernforordningen kap. III i Ingvild Sciøll Ericsons utredning for *Personvernkommisjonen*, vedlagt som digitalt vedlegg.)[116]

Barn kan likevel ikke samtykke til behandling av særlige kategorier personopplysninger før de er 18 år, jf. personvernforordningen artikkel 9 nr. 2 bokstav a. Et barn kan trolig heller ikke avgi et «uttrykkelig» samtykke etter andre bestemmelser før det er 18 år, da behandling av personopplysninger etter slike bestemmelser gjerne utgjør en høyere personvernmessig risiko enn normalt. Det er få rettskilder til belysning av spørsmålet, og forholdet til bestemmelser som krever «uttrykkelig» samtykke bør derfor avklares.

Mens vergemålsloven regulerer rettslige og økonomiske forhold, kommer barneloven til anvendelse på personlige forhold.

Det eksisterer ikke uttrykkelige bestemmelser i lovgivningen som sier noe om når barnet har selvstendig samtykkekompetanse til *deling* av personopplysninger. Datatilsynet praktiserer imidlertid «faste» aldersgrenser for når et samtykke er gyldig avgitt, uten at hjemmelen for bruken av slike aldersgrenser synes klar.[117]

Det fremgår av UNICEF sine «Guidelines for Industry on Child Online Protection» at foreldre eller foresatte spiller en aktiv rolle når det gjelder avgjørelser om hvilken informasjon og hvilket innhold barn kan få tilgang til og dele videre. Foreldrene skal også ta hensyn til barnets meninger. Ved installering av ulike filtre og «foreldrekontroller» skal foreldrene ta hensyn til barnets alder og deres evne til å kunne ta informerte valg på nettet.[118] Dette indikerer at foreldrene skal ta barnets alder i betraktning når de setter grenser for hvilket innhold barn skal få tilgang til på nett.

9.5.2.6 Foreldres rett til å eksponere egne barn

Et sentralt spørsmål er hvor langt samtykkekompetansen innenfor foreldreansvaret gir foreldrene rett til å publisere personopplysninger om egne barn. Problemstillingen var særlig diskutert i den tidligere personvernkommisjonens utredning, se NOU 2009: 1, kapittel 14.[119] Personopplysningsregelverket regulerer ikke i dag spørsmålet om hvilke opplysninger foreldre kan publisere om egne barn. Regelverket har heller ingen bestemmelser om hvorvidt Datatilsynet kan pålegge sletting av personopplysninger som foreldre har lagt ut om sine egne barn.

I høringsnotatet[120] til endringer i den forrige personopplysningsloven av 2000, gikk Justis- og beredskapsdepartementet inn på spørsmålet om foreldrenes mulighet til å samtykke på vegne av barnet. Departementet viste i den forbindelse til diskusjonen knyttet til foreldre som publiserer sensitive opplysninger om sine barn på internett. Departementet uttalte følgende, jf. punkt 8.3.2.3 side 75:

---

[114] Se nærmere om Grunnloven § 104 i kap 4 om rettslig regulering.

[115] Barnelovutvalgets forslag til ny § 6-6 viderefører § 33. Se NOU 2020: 14 *Ny barnelov – Til barnets beste*.

[116] Ericson, I. S. (2022). *Barns samtykkekompetanse på personvernfeltet*. Utredning for Personvernkommisjonen.

[117] Datatilsynet. (2022, 25. april). *Samtykke fra mindreårige.*

[118] International Telecommunication Union. (2015). *Guidelines for Industry on Child Online Protection.*

[119] NOU 2009: 1 *Individ og integritet – Personvern i det digitale samfunnet.* Fornyings- og administrasjonsdepartementet.

[120] Prop. 47 L (2011 -2012) *Endringer i personopplysningsloven.*

«Departementet bemerker at foreldreansvaret ikke er en konstant størrelse, men uttynnes gradvis, idet foreldrenes rett til å bestemme for barnet avtar etter hvert. Særlig barnets selvbestemmelsesrett etter barneloven § 33 vil kunne føre til at foreldrenes bestemmelsesrett bortfaller før barnet er 18 år.

I juridisk teori et det antatt at barnet kan ha større selvbestemmelsesrett til å nekte («nektingskompetanse») enn til å gi samtykke («samtykkekompetanse») til inngrep eller tiltak, jf. Backer: Barneloven Kommentarutgave, 2. utgave side 306 (2008). […]

Departementets foreløpige vurdering er at foreldrenes samtykkekompetanse kan begrenses på områder hvor de i utgangspunktet har slik kompetanse, både med hjemmel i nasjonal rett, jf. barneloven § 30 flg., og internasjonal rett, jf. Barnekonvensjonen. […] Samtykkekompetansen kan muligens klargjøres ved å inkorporere prinsippet om barnets beste i eventuelle særregler om behandling av barns personopplysninger, eventuelt i tillegg å innta en henvisning til barnets selvbestemmelsesrett.»

I forslaget til ny barnelov NOU 2020: 14 peker utvalget på at personvern, privatliv og personopplysninger i dag reguleres av ulike lover på ulike områder. Barnelovutvalget mente at en mangel i dagens lovgivning om personvern og privatliv er manglende oppmerksomhet om hvor langt foreldresamtykket rekker overfor barns rett til privatliv og personvern. Utvalget gikk derfor inn for å gi noen eksplisitte bestemmelser som styrker barnets rett til vern av sitt privatliv og personvern.[121] Utvalget så behov for en bestemmelse i kapitlet om foreldreansvar, som regulerer enkelte sider ved barns rett til personvern og privatliv og forholdet til foreldrenes samtykkekompetanse. Bestemmelsen ble inntatt som § 6-7 i utvalgets lovforslag. Forslaget til bestemmelse gir en plikt for foreldre til å ta hensyn til barnets rett til privatliv og personvern når de samtykker på vegne av barn, og gir aldersgrenser for når barnet oppnår selvbestemmelsesretten over personopplysninger.[122]

Etter barnelovutvalgets syn kan ikke et samtykke fra foreldrene på vegne av egne barn nødvendigvis likestilles med et samtykke fra den som opplysningen omhandler (barnet), og på den måten medføre at behovet for vern opphører.

Den nye bestemmelsen foreslås inntatt under foreldreansvaret i loven og utvalget påpeker at bestemmelsen vil være en rettslig nyvinning i barneloven.[123]

Boks 9.10 Publisering av opplysninger om egne barn i Høyesterett

I november 2019 behandlet Høyesterett for første gang problemstillingen om publisering av opplysninger om egne barn.[1] Dommen avklarer foreldreansvarets forhold til straffelovens bestemmelse om krenkelse av privatlivets fred. En mor som var i konflikt med barnevernet som følge av omsorgsovertagelse for datteren, hadde publisert bilder og videoklipp som viste datteren i sårbare situasjoner, egne referater av samtaler med datteren og brev fra barnevernet med vurderinger av datteren, på sosiale medier. Høyesterett kom, som de tidligere instanser, til at forholdet var rammet av strl. § 267. Informasjonen var klart omfattet av begrepet «privatlivets fred». Hverken datteren eller moren kunne samtykke til offentliggjøring slik at informasjonen ikke ble rettsstridig. Førstvoterende uttrykte at et eventuelt samtykke eller en aksept fra barnet selv ikke kunne ha noen betydning.[2] Straff etter strl. § 267 ville i dette tilfellet heller ikke innebære krenkelse av Grunnloven § 100, EMK artikkel 10 eller SP artikkel 19. Sistnevnte bestemmelser gjelder ytringsfrihet.

1 HR-2019-2038-A
2 HR-2019-2038-A, avsnitt 20

9.5.2.7 «Barnets beste» i møte med andre rettigheter

Spørsmålet om beskyttelse av barns privatliv og personvern aktualiserer også menneskerettigheter som kan ha kryssende hensyn. Det mest aktuelle eksempelet vil være retten til ytringsfrihet. Ytringsfriheten er blant annet beskyttet i Grunnloven § 100 og EMK artikkel 10, samt i barnekonvensjonen artikkel 13. Inngrep i ytringsfriheten

121 NOU 2020: 14 *Ny barnelov – Til barnets beste*, punkt 8.5.7.2.
122 Se nærmere NOU 2020: 14 *Ny barnelov – Til barnets beste*, kap 10 og kap 17
123 Se nærmere NOU 2020: 14 *Ny barnelov – Til barnets beste*, s. 109

kan også være tillatt etter menneskerettighetene, på nærmere bestemte vilkår.

Foreldres ytringsfrihet kan komme til utrykk ved at foreldre deler opplysninger om egne barn. Dersom myndighetene griper inn overfor en privatpersons ytringer, av hensyn til beskyttelse av andres privatliv og personvern, er dette i utgangspunktet også et inngrep i ytringsfriheten til den som deler opplysningene.

Også barn har ytringsfrihet, som kan medføre at de «utleverer seg selv» ved å legge ut innhold som gir utrykk for deres interesser, tanker og meninger.

Personvernregelverket regulerer ikke i dag spørsmålet om hva foreldre kan og ikke kan legge ut opplysninger om, eller hvorvidt Datatilsynet kan pålegge sletting av personopplysninger foreldre har lagt ut om egne barn.

9.5.3 Personvernutfordringer for barn som forbrukere

Som beskrevet gjennom dette kapitlet, har forbrukere i dag svært begrensede muligheter til å forstå omfanget av datainnsamlingen som skjer på tvers av nettsteder, apper, tingenes internett, og andre digitale tjenester. Aktørbildet er uoversiktlig, teknologien er kompleks, og avtalevilkår er vanskelig å lese og forstå. Det er umulig å ha oversikt over hvem som samler inn personopplysninger, hva opplysningene brukes til, og hvilke konsekvenser det kan ha i fremtiden. Alle disse problemstillingene aktualiseres i høyeste grad når det gjelder barns personvern.

En undersøkelse gjennomført på oppdrag fra *Personvernkommisjonen*, viser at barn og unges forståelse for personvernproblematikk varierer noe mellom aldersgrupper, men at det er generelt lav forståelse.[124] Digitaliseringen har bidratt til at forskjeller mellom by og land viskes ut, mens andre demografiske og sosiale forskjeller slik som foreldres utdanning og inntekt, skolemiljø og vennekrets påvirker kompetansen. Generelt viser undersøkelsen at barn og unge stort sett har lav bevissthet rundt personvernsproblematikk, digitale økosystemer og personvernkonsekvenser ved bruk av digitale tjenester.

Det er også en generelt lav forståelse av hvordan man kan ivareta eget personvern. Mange av barna som ble intervjuet har en anelse om at noen «kikker dem over skulderen», særlig blant de eldste, men de har vanskeligheter med å sette fingeren på hvorfor dette skjer. Undersøkelsen tyder også på at bevisstheten er større rundt personvern knyttet opp mot andre barn og andre brukere, enn knyttet til tjenestetilbyderne. Som beskrevet ovenfor, er verdikjedene, teknologien og avtalevilkårene som ligger til grunn for mye av databehandlingen svært komplisert, og ofte umulig å forstå også for voksne. Dette tilsier at barn heller ikke har anledning til å forstå disse komplekse systemene og spørsmålene, og at det ikke er hensiktsmessig å forvente en slik forståelse.

> *«Jeg likte ikke TikTok. Jeg syns det var ubehagelig at alle plutselig kunne se på meg»*
>
> *Jente, 10*[125]

I rapporten «Photoshop, fillers og falske glansbilder?» fra 2019 kommer det fram at ungdommer (15–20 år) forstår at informasjon som legges ut i sosiale medier brukes av tredjeparter for å skreddersy innhold. Ungdommene er klare over at algoritmer brukes til blant annet atferdsbasert markedsføring. Flere oppgir at de synes det er ubehagelig å føle at man overvåkes i digitale tjenester, men føler på en resignasjon fordi de ofte føler at de ikke har noe annet valg enn å samtykke til innhenting av personopplysninger.[126] Dette tyder på at selv om forståelsen for at personopplysninger samles inn og brukes til uønskede formål øker med alderen, fører ikke dette til en tilsvarende økning i handlekraft for å ivareta personvernet. Det vitner om en personvernresignasjon også blant unge.

Undersøkelsen viser også at barn «var eksponert for mye «problematisk» markedsføring i sine sosiale medieprofiler, som for eksempel alkohol, gambling og kosmetiske behandlinger».[127] Markedsføringen var i «betydelig grad skreddersydd» etter barns «personlige data som kjønn, lokasjon, alder, etnisitet og digitale aktiviteter».[128] De vanligste markedsføringsteknikkene var sponsede lenker, kjendissponsing og rabattkoder.

I Storbritannia har myndighetene utformet bindende retningslinjer som har til hensikt å beskytte barn på nett. Retningslinjene «Age

[124] Falch, C. (2022). *Rapport til Personvernkommisjonen. Intervjuer med barn og unge om personvern.*

[125] Steinnes, K.K., Teigen, H.F. & Bugge, A.B. (2019). *Photophop, fillers og falske glansbilder? En studie blant ungdom om kjønn, kropp og markedsføring i sosiale medier.* Forbruksforskningsinstituttet SIFO, OsloMet.

[126] Steinnes, K.K., Teigen, H.F. & Bugge, A.B. (2019). *Photophop, fillers og falske glansbilder? En studie blant ungdom om kjønn, kropp og markedsføring i sosiale medier.* Forbruksforskningsinstituttet SIFO, OsloMet.

[127] OR 13 – 2018 Barn og unge sosiale medier (1).pdf

[128] OR 13 – 2018 Barn og unge sosiale medier (1).pdf side 10

Appropriate Design Code» trådte i kraft i 2020, og stiller en rekke krav til virksomheter som tilbyr tjenester som brukes av barn.[129] Alle tjenesteleverandører som har barn blant sine brukere er lovpålagt å følge retningslinjene, tjenesten trenger ikke nødvendigvis å være rettet spesifikt mot barn og unge. Brudd på retningslinjene kan medføre sanksjoner fra det britiske datatilsynet.

De bindende retningslinjene fremsetter 15 standarder som må følges av aktører som tilbyr tjenester som brukes av barn. Det inkluderer blant annet krav om å ta hensyn til barnets beste, gjennomføring av personvernkonsekvensvurderinger, en risikobasert tilnærming når en vurderer brukernes alder, personvernvennlige standardinnstillinger, gjennomsiktighet og informasjon tilpasset barn, samt verktøy for å hjelpe barn å ivareta sine personvernrettigheter. Etter introduksjonen av retningslinjene, innførte flere store plattformer globale endringer for å bedre ivareta barns personvern.[130] Et lovforslag inspirert av de britiske retningslinjene ble lagt fram av myndighetene i California i 2022.[131]

9.5.3.1 Atferdsbasert markedsføring mot barn

For mange næringsaktører er barn og unge en populær målgruppe, og som et følge av dette utsettes barn ofte for store mengder markedsføring og kommersielt press.[132] Mange av de mest populære digitale tjenestene som benyttes av barn er reklamefinansierte, og atferdsbasert markedsføring kan rettes mot barn så vel som mot voksne.

Barn har generelt vanskeligere for å forstå markedsføring enn voksne, inkludert en lavere evne til å kjenne igjen markedsføring, skille dette fra annen kommunikasjon, samt å forstå markedsførerens hensikt.[133] Det blir desto vanskeligere å identifisere markedsføring dersom det er integrert i underholdnings- eller annet innhold, for eksempel ved at influensere promoterer produkter[134] eller at spill blir en del av en markedsføringskampanje.[135]

Forbrukertilsynet fremhever at digital markedsføring foregår på måter og i kanaler hvor det er vanskelig for foreldre å holde oversikt. Markedsføringen kan tilpasses barnets alder og andre individuelle trekk, og selv om foreldrene er til stede på de samme plattformene og tjenestene vil ikke de bli eksponert for de samme annonsene.[136] Dersom markedsføringen er atferdsbasert og tilpasset segmenter eller individer, blir det nesten umulig for foreldre og tilsynsmyndigheter å vite hvilke annonser barna ser.

Gruppen Reset Australia har blant annet avdekket at Meta tillater virksomheter å reklamere mot barn helt ned i 13 års alder som har utrykt interesse for røyking, ekstrem vektreduksjon og gambling.[137] I Norge har Forbrukerrådet avdekket at apper rettet mot små barn drives av reklamenettverk,[138] og at digitale produkter som leker og GPS-klokker rettet mot barn mangler grunnleggende personvern.[139]

Det kan også være problematisk dersom barns personopplysninger benyttes til å tilpasse og/eller målrette innhold utover markedsføring. Barn kan for eksempel være særlig sårbare for påvirkning gjennom desinformasjon og ytterliggående innhold. Dette har blitt aktualisert gjennom tilfeller hvor anbefalingsalgoritmer har anbefalt ekstremt, radikaliserende eller misvisende innhold til barn.[140]

Som omtalt i avsnitt 9.4.2, har både Europaparlamentet og Regjeringen inntatt en posisjon om at atferdsbasert markedsføring mot barn bør forbys som en del av den kommende forordningen om digitale tjenester (DSA). Det argumenteres med at barn er særlig sårbare for denne typen markedsføring.

Det er foreløpig ikke klart hvordan tjenesteleverandører kan vurdere om en bruker er et barn eller ikke. Det er grunn til å anta at brukere av en app myntet på treåringer i hovedsak vil være barn. Denne vurderingen vil være vanskeligere dersom en tjeneste har innhold myntet på både barn, tenåringer og voksne. Dersom tjenesteleverandører pålegges å verifisere alder og identitet på samtlige brukere, kan dette ha uheldige konsekvenser for

---

[129] Information Commissioner's Office. (2020). *Age appropriate design: a code of practice for online ser.*

[130] The Guardian. (2021, 5. september). *Social media giants increase global child safety after UK regulations introduced.*

[131] Financial Times. (2022, 16. februar). *California to adopt UK-style child data law in global push against Big Tech.*

[132] NOU 2011: 20 *Ungdom, makt og medvirkning.*

[133] Forbrukertilsynet. (u.å.). *Forbrukertilsynets veiledning om handelspraksis overfor barn og unge.*

[134] Forbrukerrådet. (2019, 28. februar). *Ung og utsatt for usunn reklame.*

[135] BEUC. (2021). *TikTok without filters.*

[136] Forbrukertilsynet. (u.å.). *Forbrukertilsynets veiledning om handelspraksis overfor barn og unge.*

[137] The Guardian. (2021, 28. april). *Facebook allows advertisers to target children interested in smoking, alcohol and weight loss.*

[138] Forbrukerrådet. (2020). *Out of control*, s. 77.

[139] Forbrukerrådet. (2018, 5. mai). *Krever trygge IoT-produkter for barn.*

[140] Mozilla. (2021). *YouTube Regrets: A crowdsourced investigation into YouTube's recommendation algorithm.*

personvernet, fordi det kan føre til at flere personopplysninger må behandles.[141]

9.5.3.2 Barns personvern og andre rettigheter

Bruken av personopplysninger for å styre barns tilgang på informasjon kan påvirke barns autonomi og muligheter til å kunne utvikle seg. Det er problematisk dersom algoritmiske systemer som drives av globale teknologiselskaper får stor makt til å forme barn og unges verdensbilde og virkelighetsoppfatning. I sin generelle kommentar uttaler FNs barnekomité blant annet at automatiserte systemer ikke bør brukes for å påvirke barns oppførsel eller følelser, eller for å begrense deres muligheter og utvikling.[142]

Personvernkommisjonen mener barn ikke skal settes i situasjoner hvor de må gi opp retten til personvern for å kunne utøve øvrige rettigheter. Barns personvern må ivaretas i digitale tjenester på en måte som gjør at de kan utøve andre rettigheter, som retten til meningsdannelse, sosialt samvær og informasjonssøk. Personvernet skal ikke være en hindring for disse rettighetene, men må være komplementært.

9.5.3.3 Foreldres ansvar for utlevering av barns personopplysninger

I tillegg til å møte personvernutfordringer fra kommersielle aktører, er barn også utsatte forbrukere i møte med foreldre og andre barn. Uønsket bildedeling er for eksempel noe som har blitt viet mye oppmerksomhet, både gjennom at foreldre og besteforeldre legger ut bilder i sosiale medier, eller ved at barn deler bilder av hverandre som en del av mobbing på nett. Ifølge rapporten EU Kids Online 2018 utført i Norge, har fem prosent av alle barn hatt negative erfaringer regelmessig (hver måned) på internett, mens 17 prosent har hatt dette noen få ganger.[143]

Publisering av bilder og personopplysninger i sosiale medier aktualiserer flere juridiske problemstillinger, herunder avveininger av ulike rettigheter. Forholdet mellom ytringsfriheten og privatlivet står sentralt ved publisering av opplysninger om andre. Disse rettighetene kan komme i et spenningsforhold. I tilfeller der foreldre publiserer opplysninger om egne barn kompliseres dette ytterligere ved at det i tillegg er særlige prinsipper og regler som gjør seg gjeldende.

Ifølge FNs barnekonvensjon, samt i den allmenne samfunnsoppfatningen, er det foreldrene som har hovedansvaret for barnets omsorg og utvikling, i tråd med det som er best for barnet. Foreldrene har et oppdrager- og opplæringsansvar overfor barna sine. De har ansvaret for om aldersgrenser for tilgang til ulike plattformer overholdes og om de gir samtykke for yngre barn. Foreldrene har ansvaret for barnets personvern, liv og helse knyttet til den digitale verden. Barnet skal beskyttes mot det som kan være skadelig. Samtidig kan foreldre selv krenke barns rettigheter gjennom sin egen digitale atferd. Det innebærer at foreldre må være bevisste på konsekvensene av å dokumentere og dele barns barndom på nett.

9.5.3.4 Foreldres deling av bilder av barn

De seneste årene har det oppstått en delingskultur, hvor foreldre deler bilder og videoer helt fra første ultralyd til siste skoledag. Slik praksis setter digitale spor knyttet til det enkelte barn, som barnet selv ikke har kontroll over. Slik kan foreldrene være med på å skape en digital identitet som barnet selv, når det vokser opp, ikke ønsker eller kjenner seg igjen i. Dette kan utfordre barns rett til personvern.

Ifølge resultater fra undersøkelsen EU Kids Online 2018, oppgir 33 prosent av norske barn at deres foreldre eller foresatte har delt informasjon om dem på nettet uten å først ha spurt dem om det var greit.[144] Dette er klart høyest blant de 19 landene som har vært med i undersøkelsen.

Selv om en forelder for eksempel kan synes et bilde av barnet er fint, kan det hende at barnet selv er uenig. Som forklart ovenfor har barnet med- og selvbestemmelsesrett etter barneloven. Barns gryende forståelse av hvordan de oppfatter seg selv, og ikke minst at de litt etter litt skal lære om sine rettigheter knyttet til bilder og opplysninger om dem selv, er sentralt i en verden der innhold produseres og deles som aldri før. De yngste barna har ingen forutsetning for å forstå hva internett og deling i sosiale medier er, og derfor er særlig sårbare.

---

[141] The Guardian. (2022, 13. februar). *Plans for age checks on porn sites 'a privacy minefield', campaigners warn.*

[142] United Nations. (2021, 2. mars). *General comment No. 25 (2021) on children's rights in relation to the digital environment.* Convention on the Rights of the Child. Committee on the Rights of the Child.

[143] Staksrud, E. & Ólafsson, K. (2019). *Tilgang, bruk, risiko og muligheter, Norske barn på Inter Resultater fra EU Kids Online-undersøkelsen i Norge 2018.*

[144] Staksrud, E. & Ólafsson, K. (2019). *Tilgang, bruk, risiko og muligheter, Norske barn på Inter Resultater fra EU Kids Online-undersøkelsen i Norge 2018.*

Å styrke barns forståelse av personvern og gi dem gode vaner allerede i tidlig alder, er et viktig bidrag i arbeidet for et godt psykososialt læringsmiljø i barnehage og skole. Et barn som har kjennskap til rettighetene sine, vil lettere kunne sette egne grenser – og respektere andres. Dersom foreldre er respektfulle i omgangen sin med bilder, vil barnet lære av dem. Det innebærer også å ta barns meninger på alvor.

Foreldre har både foreldreansvar og ytringsfrihet, mens barna på sin side har rett til privatliv. Omfattende eksponering vil kunne innebære en krenkelse av barns rett til privatliv. Dette kan eksempelvis være opplysninger i tilknytning til en barnevernssak, helseopplysninger eller opplysninger om barnet fra rettsdokumenter.[145]

Barn er i stadig utvikling, og bilder som ble delt uten motforestillinger på et tidspunkt, kan oppleves ugreit senere. Datatilsynets veileder «I beste mening» forklarer hvilke prinsipper som bør gjelde før man eventuelt legger ut bilder av barn på nett. Tilsynet anbefaler å begrense delingen av barnebilder, alltid spørre barnet om det er greit, samt å slette delte bilder etter hvert.[146]

Et annet spørsmål er der andre familiemedlemmer publiserer opplysninger om barn. Denne personkretsen kan også potensielt krenke barns rett til personvern. Andre personer som ikke har foreldreansvaret, bør normalt ha en mer innskrenket adgang til å eksponere barn, på linje med andre utenforstående.

Barn kan også ha stor påvirkning på hverandres personvern, gjennom å dele og/eller legge ut informasjon om andre barn. Dette har blant annet fått mye oppmerksomhet i kontekst av mobbing på nett og spredning av nakenbilder. Digitale tjenester har gjort terskelen lav for å kunne spre innhold uten tillatelse, og dersom innhold først er spredt kan det være umulig å få slettet det.[147]

I tilfeller hvor et barn sprer bilder av seg selv eller av andre barn, vil det ofte skyldes at barnet ikke forstår de mulige konsekvensene av slik spredning. Dette er utfordringer som mulig kan forebygges ved opplæring i barnehage og skole, som beskrevet i kapittel 8.

Personvernkommisjonen anbefaler at personvernutfordringer knyttet til innhold delt av foreldre og andre barn forebygges gjennom kompetanseheving, blant annet gjennom undervisning. Dette er et område hvor tiltak knyttet til nettvett og vurderingsevne er viktig.

9.5.3.5 Foreldres kommersielle eksponering av barn i sosiale medier

Som nevnt bruker mange foreldre sosiale medier til å legge ut bilder av barna sine. Dette kan i seg selv være ulovlig med hensyn til innhold. De siste årene har det utviklet seg en trend hvor noen foreldre bruker egne barn i sosiale medier, med kommersielt formål. Formålet med kommersiell bruk av barn i sosiale medier er å tjene penger eller få sponsede produkter, mens formålet i andre tilfeller gjerne vil være å dele bilder av barna med venner og familie og/eller få bekreftelse eller oppmerksomhet gjennom kommentarer og «likes».

I praksis foregår dette ofte ved at foreldrene inngår en avtale med en kommersiell aktør (nettbutikk eller annet) om at de (foreldrene og barnet) skal være ambassadører for aktøren, eller ved at foreldrene blir betalt i form av penger for å vise frem klær og utstyr hvor barna blir brukt som modeller. Foreldrene publiserer deretter bilder av barnet med det aktuelle produktet og sier noe positivt om det produktet i sosiale medier. I slike tilfeller offentliggjør foreldrene personlig informasjon om barnet sitt (for eksempel bilde av barnet) for å reklamere for produkter de har fått. Som ved foreldres deling av bilder av barn for øvrig, er det problematisk for barns personvern at personopplysninger om dem offentliggjøres. Det er særlig problematisk når det er sterke kommersielle insentiver for å eksponere barn.

Personvernkommisjonen mener foreldre ikke bør publisere barns personopplysninger, inkludert bilder, for kommersielle formål på nett.

9.5.3.6 Foreldres overvåkning av barn

Foreldre kan også påvirke barns personvern i negativ retning ved å anvende digital teknologi for å følge med på og/eller overvåke barna. Den digitale utviklingen har medført mange nye muligheter for foreldre som ønsker å holde et øye med sine barn i forskjellige kontekster. Et eksempel er funksjoner i sosiale medier som lar brukere se hverandres lokasjon, for eksempel gjennom funksjonen SnapMap i den populære tjenesten SnapChat, eller gjennom bankapplikasjoner som lar foreldre overvåke kjøpsaktivitet.[148]

Utbredelsen av tingenes internett har også lagt til rette for en rekke nye verktøy som kan bru-

---

[145] NOU 2009: 1 *Individ og integritet – Personvern i det digitale samfunnet* s. 138.

[146] Datatilsynet. (2020). *I beste mening: Bilder av barn på nett.*

[147] Barneombudet. (2019). *Ungdom om digitale medier. Vurderinger og forslag fra Barneombudets ekspertgruppe om en tryggere digital hverdag.*

kes for å spore og lytte inn på barn. Eksempelvis har GPS-klokker for barn blitt markedsført som sikkerhetsverktøy som lar foreldre holde bedre oversikt over hvor barna befinner seg, og som alternativer til mobiltelefoner for de yngste barna. Slike klokker har blitt relativt populære i Norge blant foreldre som ønsker ekstra sikkerhet i hverdagen.[149]

I 2017 avdekket Forbrukerrådet at flere populære typer GPS-klokker for barn solgt i Norge, hadde alvorlige sikkerhetsmangler som gjorde det mulig for fremmede å overvåke barnet.[150] Datatilsynet og Barneombudet har også advart mot å bruke slike produkter, blant annet på grunn av nedkjølingseffekten denne typen overvåkning kan ha på barn, for eksempel ved at de unngår situasjoner som er en vanlig del av barns utviklingsløp fordi de vet at foreldrene følger med. Ifølge Datatilsynet og Barneombudet kan bruken av sporingsteknologi på barn skape unødvendig frykt, og ha negative effekter på barns utvikling fordi de ikke lærer å håndtere utfordringer på egen hånd.[151] Kontinuerlig overvåkning av barn kan også ha en negativ effekt på tillitsforholdet mellom barn og foreldre.[152]

I 2021 utarbeidet FNs barnekomité en General Comment no. 25 om artikkel 16.[153] Kommentaren tar blant annet opp krenkelser mellom barn og foreldre, og advarer mot rutinemessig overvåkning av barn og unge.

I en spørreundersøkelse gjennomført av Datatilsynet kom det fram at mer enn tre av fire respondenter mener det er uakseptabelt å spore barn og tenåringer i det daglige liv.[154] Respondentene mener imidlertid at det er mer akseptabelt å spore de minste barna, enn barn over tolv år. Generelt kom det fram av undersøkelsen at de under 30 år er mer kritiske til at foreldre overvåker barna sine enn de over 30 år. Det kan tyde på at de som selv har vokst opp med digitale tjenester er mest skeptiske til sporing og «snoking» i barns digitale liv.

FNs barnekonvensjon sier: *«Alle barn har rett til eit privatliv.»* Barneombudet tolker dette slik at foreldre vanligvis ikke har lov til å lese barnets e-poster, dagbok eller for øvrig snoke i barnets ting.[155] Dersom foreldrene har god grunn til å tro at barnet er i ferd med å bli utsatt for noe skadelig eller skader andre, mener Barneombudet at foreldrene likevel kan sjekke barnets private ting.

Personvernkommisjonen mener at selv om bruken av digitale verktøy for å overvåke barn kan gi en økt følelse av trygghet og kontroll for både barn og foreldre, kan dette være inngripende i barnets rett til personvern.

Personvernkommisjonen mener Barneombudet bør utvikle en veileder for barn og foreldre for å styrke forståelsen av barns rett til personvern i familiære forhold.

9.6 Personvernkommisjonens anbefalinger oppsummert

Forbrukers mulighet til å ivareta eget personvern

- *Personvernkommisjonen* anbefaler at Regjeringen fører en offensiv personvernpolitikk opp mot EU.
- *Personvernkommisjonen* anbefaler at Regjeringen tar initiativ til å utrede hvordan teknologi kan brukes til å beskytte forbrukerne, for eksempel gjennom personvernvennlige standardinnstillinger eller automatisk blokkering av illegitim sporing. Det er vesentlig at det offentlige tar et slikt initiativ, slik at det ikke utelukkende er de globale plattformaktørene som i praksis leder an i dette arbeidet.

Tilsyn og håndheving

- *Personvernkommisjonen* anbefaler at ansvaret for håndheving av bruk av informasjonskapsler og lignende sporingsteknologi legges til Datatilsynet.
- *Personvernkommisjonen* mener Regjeringen bør støtte et forslag om en kommunikasjonsvernforordning som stiller krav til bruk av sporingsteknologi som er i samsvar med personvernforordningen.

[148] Falch, C. (2022). *Rapport til Personvernkommisjonen. Intervjuer med barn og unge om personvern*, s. 33.

[149] NRK. (2017, 6. januar). *Salget av mobilklokker til barn tok av før jul tross advarsel.*

[150] Forbrukerrådet. (2017, 18. oktober). *Elendig sikkerhet i GPS-klokker for barn.*

[151] P4. (2022, 27. april). *Kritisk til GPS-overvåking av barn.*

[152] Rooney, T. (2010). Trusting children: How do surveillance technologies alter a child's experience of trust, risk and responsibility. *Surveillance and Society, 7*(3/4), 344-355.

[153] Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, 2. march 2021.

[154] Datatilsynet & Teknologirådet. (2015). *Personvern 2015 – Tilstand og trender.*

[155] Barnekonvensjonen i enkel versjon – Barneombudet

Lovprosesser i EU

- *Personvernkommisjonen* anbefaler at Regjeringen engasjerer seg i utformingen av forordningen for kunstig intelligens med vedlegg, og jobber for en regulering som sørger for at KI-systemer utformes på en måte som ivaretar personvernet i både utvikling og bruk av systemene.
- *Personvernkommisjonen* anbefaler at Regjeringen støtter Europakommisjonens forslag om en horisontal IKT-sikkerhetslov (Cyber Resilience Act).
- *Personvernkommisjonen* mener Regjeringen bør være en aktiv pådriver i EUs lovgivingsprosesser som berører forbrukernes personvern.

Tingenes internett

- *Personvernkommisjonen* anbefaler at norske importører, forhandlere og bransjeorganisasjoner har informasjon tilgjengelig om hvordan personvernet ivaretas før salg av tilkoblede produkter.
- *Personvernkommisjonen* anbefaler at forhandlere har kontrollrutiner på plass for å sikre at produkter som selges i Norge opererer i tråd med personvernregelverket og ekomloven, og stiller krav til sine leverandører knyttet til blant annet dataminimering, formålsbegrensning og personvern som grunninnstilling. Bransjestandarder og merkeordninger kan være et viktig verktøy for å sørge for at leverandørene ivaretar slike krav.
- *Personvernkommisjonen* anbefaler at Regjeringen har som posisjon i regelverksutvikling at forhandlere får et rettslig ansvar for manglende IKT-sikkerhet og personvern i produkter de selger.

Atferdsbasert markedsføring

- *Personvernkommisjonen* deler Regjeringens syn på at atferdsbasert markedsføring mot barn bør forbys. *Kommisjonen* støtter også at bruken av særlige kategorier av personopplysninger til markedsføringsformål forbys. Forbudet bør også gjelde særlige kategorier av personopplysninger som er utledet fra data som ikke var sensitive ved innsamlingspunktet, for eksempel lokasjonsdata som sammenstilt kan avdekke politisk eller religiøs tilhørighet.
- *Personvernkommisjonen* anbefaler at ved et forbud mot adferdsbasert markedsføring som kun gjelder barn, må tjenesteleverandører pålegges et føre var-prinsipp. Det er ikke ønskelig med løsninger som fører til økt sporing og profilering for å kartlegge forbrukeres identitet og alder.
- *Personvernkommisjonen* anbefaler videre at *bruk av* barns personopplysninger til atferdsrettet markedsføring bør forbys. Barns personopplysninger bør ikke anvendes til atferdsrettet markedsføring, selv dersom markedsføringen ikke rettes mot barn.

Personvernkommisjonen har delt seg i et flertall og et mindretall i spørsmålet om et *generelt forbud* mot atferdsbasert markedsføring bør utredes:

- *Personvernkommisjonens flertall, medlemmene Busch, Grande, Haugli, Hertzberg, Høyer, Myrstad, Schartum, Veum, Ytre-Arne og Aasberg*, ønsker å fremheve at atferdsbasert markedsføring også kan være skadelig for befolkningen for øvrig. Av den grunn mener *kommisjonens flertall* at det bør utredes hvorvidt et generelt forbud er nødvendig for å beskytte norske og europeiske forbrukere. En slik utredning bør se på hvilke positive og negative konsekvenser et slikt forbud vil ha i Norge og i Europa, blant annet for medieindustrien.
- *Personvernkommisjonens mindretall, medlemmene Moen og Næss*, anser at atferdsbasert annonsering kan gjøres på ulike måter – forsvarlig og uforsvarlig. Medlemmene Moen og Næss mener at så lenge atferdsrettet markedsføring gjøres forsvarlig vil et generelt forbud være uforholdsmessig. Moen og Næss støtter derfor ikke flertallets forslag om at det bør utredes hvorvidt et generelt forbud er nødvendig.

Åpenhet og informasjon

- *Personvernkommisjonen* anbefaler at det stilles strenge informasjons- og åpenhetskrav til hvordan forbrukerne profileres og segmenteres ved målretting av annonser og politiske budskap. Det innebærer at næringsdrivende, organisasjoner og politiske partier er åpne angående hvilke budskap de sender ut, og hvem de forsøker å nå med budskapene. Plattformer som tilrettelegger for segmentering og profilering av forbrukerne bør også tilby verktøy for å vise hvilke annonser som vises på plattformen, og hvilke segmenter de bruker. Åpenhet er nødvendig for å avdekke urimelig eller skadelig påvirkning. Regjeringen bør arbeide for å få på plass slike krav gjennom EU.

Manipulerende design

- *Personvernkommisjonen* mener et forbud mot manipulerende design, som foreslått i DSA, vil styrke forbrukeres muligheter til å ivareta eget personvern på nett. Et slikt forbud bør kompletteres med håndheving av gjeldende forbrukerregelverk, samt med veiledere fra tilsynsmyndighetene som tydeliggjør grensedragningen mellom hva som vurderes som henholdsvis akseptabel og uakseptabel bruk av design. Et slik forslag bør forankres og sikres gjennom EU-samarbeidet.

Profilering, segmentering og diskriminering

- *Personvernkommisjonen* anbefaler at Likestillings- og diskrimineringsombudet bør samarbeide med Datatilsynet om å motvirke diskriminering som et følge av bruk av maskinlæringssystemer.
- *Personvernkommisjonen anbefaler* at virksomheter som bruker maskinlæringssystemer for å profilere og segmentere forbrukere bør rapportere hvordan de motvirker diskriminerende effekter i systemene. Offentlige myndigheter bør stille krav om slik rapportering ved anskaffelser og bevilgning av midler. Regjeringen bør arbeide for at slike krav blir en del av den kommende forordningen for kunstig intelligens og dets vedlegg.

Oljefondets investeringer

- *Personvernkommisjonen* anbefaler at det stilles krav til ivaretakelse av personvernet, i likhet med krav som stilles til ivaretakelse av andre grunnleggende menneskerettigheter, når Oljefondet investerer i teknologiselskaper.
- *Personvernkommisjonen* anbefaler at Oljefondet avstår fra å investere i selskaper som krenker personvernet, og som det ikke har mulighet til å påvirke, for eksempel på grunn av majoritetseiere.

Konkurranse

- *Personvernkommisjonen* anbefaler at Norge tar initiativ til, og leder, et internasjonalt arbeid for å utrede hvordan virkemidler i konkurranseloven kan anvendes for å forhindre negative personvernkonsekvenser ved oppkjøp og fusjoner. Utredningen må vurdere om konkurranseloven er innrettet slik at den kan håndtere utfordringene i dataøkonomien på en effektiv måte. Dette må også sees i forbindelse med innføringen av nye konkurranseverktøy under den kommende forordningen om digitale markeder (DMA).
- *Personvernkommisjonen* mener offentlige myndigheter bør stimulere til utvikling av løsninger og standarder for dataportabilitet og teknisk interoperabilitet. Forekomsten av slike løsninger er en forutsetning for sunn konkurranse i mange digitale vare- og tjenestemarkeder.
- *Personvernkommisjonen* mener det er en grunnleggende forutsetning for godt personvern at det skal straffe seg å bryte loven. Effektiv håndhevelse av personvernregelverket er derfor nødvendig for å etablere like spilleregler, og for å stimulere til innovasjon innenfor personvernfremmende teknologi.
- *Personvernkommisjonen* mener det er problematisk for personvernet at norske selskaper og globale teknologigiganter ikke opererer under like konkurransevilkår. Regjeringen må ta grep for å begrense gigantenes markedsmakt for å sikre like spilleregler, og slik tilrettelegge for innovasjon som støtter opp under personvernet.

Særlig om barns personvern

- *Personvernkommisjonen* anbefaler at Regjeringen nedsetter et lovutvalg for å gjennomgå og foreslå endringer i regelverk for å beskytte barn og unge i digitale flater.
- *Personvernkommisjonen* anbefaler at personvernutfordringer knyttet til innhold delt av foreldre og andre barn forebygges gjennom kompetanseheving, blant annet gjennom undervisning. Dette er et område hvor tiltak knyttet til nettvett og vurderingsevne er viktig.
- *Personvernkommisjonen* mener Barneombudet bør utvikle en veileder for barn og foreldre for å styrke forståelsen av barns rett til personvern i familiære forhold.

Del III
Andre områder kommisjonen har arbeidet med

Kapittel 10
Regelkompleksitet og nasjonalt handlingsrom

10.1 Innledning

Et felles europeisk regelverk om personvern er viktig og verdifullt. *Personvernkommisjonen* konstaterer at europeisk og internasjonal regulering er en forutsetning for effektiv regulering av personopplysninger i en global økonomi. Den sosiale, økonomiske, forvaltningsmessige, kulturelle og politiske integrasjonen i Europa gjør felles regelverk for vern av personopplysninger og personlig integritet spesielt viktig. Det er imidlertid også utfordringer ved regelverket, særlig knyttet til kompleksitet.

I dette kapitlet gir *Personvernkommisjonen* oppmerksomhet til utfordringer regelverkskompleksitet skaper. Hovedtemaet er hvordan problemene kan reduseres ved å bruke norsk, nasjonal lovgivning for å tydeliggjøre og supplere de felles europeiske bestemmelsene («nasjonalt handlingsrom»).

10.2 Et viktig, men vanskelig regelverk

Forståelige personvernregler har betydning på alle samfunnsområder. Det handler om regelverk som skal sikre grunnleggende rettigheter og friheter, blant annet ved å gi rettigheter til det enkelte menneske. Personvernregelverket er stort og komplisert, og er for en stor del skrevet på et språk som er vanskelig å forstå – ikke bare for innbyggere flest, men også for eksperter. Omfattende og vanskelig forståelige regelverk er ikke noe nytt fenomen, hverken innen EØS-retten eller i norsk, nasjonal rett. *Personvernkommisjonen* mener likevel utfordringene slike regler skaper bør få oppmerksomhet.

Det er flere forhold som gjør personvernregelverket vanskelig å få oversikt over og forstå. Her vil *Personvernkommisjonen* nøye seg med å nevne noen viktige, utvalgte forklaringer.

Finne riktig regelverk

En fordel med personvernforordningen er at den har et meget bredt virkeområde. En kan derfor ofte gå ut ifra at dette regelverket gjelder. Samtidig gjelder ikke forordningen alltid, og det kan være vanskelig å avgjøre når det er annet regelverk som får anvendelse. Dette gjelder særlig grensegangen mellom personvernforordningen og direktivet om beskyttelse av fysiske personer ved behandling av personopplysninger for å forebygge, etterforske, avdekke eller strafforfølge lovbrudd eller gjennomføring av straffereaksjoner om fri utveksling av slike opplysninger («politidirektivet»), samt forholdet mellom personvernforordningen og EU-regulering av personvern på særskilte områder. Videre er det innen helseområdet flere særnorske lover som gjelder behandling av helseopplysninger, der det kan være vanskelig å forstå hvilken lov som kommer til anvendelse.

Forstå forholdet mellom regelverk

Ofte gjelder flere regelverk om personvern samtidig. Dette gjelder både EU-rettslig regelverk og nasjonal lovgivning. I mange tilfeller må en forstå sammenhengene mellom generelt og særskilt EU-regelverk og én eller flere norske, nasjonale lover og forskrifter. Selv om rettsreglene ikke kommer i strid med hverandre, vil det i mange tilfeller herske usikkerhet om hvordan regelverkene skal forstås i sammenheng. Et aktuelt eksempel er forslaget til forordning om kunstig intelligens (KI).[1] KI-systemer vil meget ofte innebære behandling av personopplysninger. I tillegg vil resultatene slike systemer gir, kunne ha stor betydning for personvernet. Selv om forholdet mellom forslaget til KI-forordning og personvernforordningen er meget

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, Brussel, 21. april. 2021 COM (2021) 206 final.

nært, har EU i sitt utkast til forordning unnlatt å avklare mange av spørsmålene som oppstår om hvordan regelverkene henger sammen. Lignende situasjoner oppstår når en skal prøve å forstå sammenhengen mellom personvernforordningen og norsk nasjonal lovgivning, for eksempel helselovgivningen.

Omfang og intern struktur

Personvernregelverket er meget omfattende. Personvernforordningen alene består av 99 artikler som skal leses i lys av 173 fortalepunkter, uten at det er klare henvisninger, hverken mellom artiklene eller fortalepunktene. Den vage og skjønnsmessige formuleringen mange av bestemmelsene har, gjør dessuten at det oppstår mange mulige sammenhenger mellom dem. Det krever derfor stor grad av profesjonalitet å se de sammenhenger og muligheter regelverket gir. Jo bedre en kjenner bestemmelsene, dess mer kan en derfor få ut av dem.

Kompleksiteten og de vage, skjønnsmessige formuleringene som preger mange bestemmelser skaper et sterkt behov for god veiledning. Dette blir gjort nærmere rede for i avsnitt 10.3.2.

For behandlingsansvarlige og den enkelte registrerte person, er det således kapitlene 1–5 i personvernforordningen, samt enkelte bestemmelser i øvrige kapitler, som har størst betydning. Andre deler av de ti kapitlene i forordningen, har mest betydning for tilsynsmyndigheter og nasjonale lovgivere.

Bestemmelser om registrertes rettigheter er samlet i personvernforordningens kapittel 3. Det kan imidlertid være vanskelig å forstå hva rettighetene spesifikt går ut på. Ønsker man for eksempel å finne ut av hvilke krav som stilles til samtykke, innebærer fraværet av klare strukturer og henvisninger at man må lete seg frem til artiklene 4 nr. 11, 6 nr. 1, 7, 8 og 9 nr. 2 bokstav a, og forstå den nærmere relasjonen mellom disse bestemmelsene. I mange tilfeller må den som anvender bestemmelsene dessuten være klar over at samtykke også kan gjelde annet enn i personvernforordningen. Å samtykke til behandling av personopplysninger skiller seg eksempelvis fra å samtykke til unntak fra taushetsplikt etter forvaltningsloven eller å samtykke til medisinsk behandling etter pasient- og brukerrettighetsloven.

I andre tilfeller gir personvernforordningen en enkel hovedregel, kombinert med unntaksregler det nesten er umulig å være sikker på betydningen av. En hovedregel om sletting av personopplysninger er for eksempel at opplysningene «ikke lenger er nødvendige for formålet som de ble samlet inn eller behandlet for».[2] Det blir imidlertid atskillig vanskeligere når en skal ta stilling til betydningen av unntakene fra denne hovedregelen. Det kan for eksempel gjøres unntak fra hovedregelen om sletting dersom fortsatt behandling av personopplysningene er nødvendig for «arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1 i den grad rettigheten nevnt i nr. 1 sannsynligvis vil gjøre det umulig eller i alvorlig grad vil hindre at målene med nevnte behandling nås».[3] Slike sterkt skjønnsmessige bestemmelser gir god mulighet for argumentasjon, men sjelden grunnlag for sikre konklusjoner. Det er mange slike krevende skjønnstemaer i personvernregelverket.

Språk

Hver bestemmelse (artikkel) i personvernforordningen er ofte ordrik og skrevet i lange og komplekse setningsstrukturer på opptil 50 ord i én setning.[4] Regelstrukturen er ofte kompleks, for eksempel slik at en hovedregel er etterfulgt av flere unntak, hvoretter det er stilt opp vilkår for å gjøre unntak fra unntakene.[5]

Språket i personvernforordningen er preget av en rekke begreper der meningsinnholdet er fastlagt i egne regler (legaldefinisjoner). Begrepsinnholdet er ofte komplekst og vagt/skjønnsmessig. Det er nødvendig å huske definisjonene når de aktuelle ordene forekommer i regelteksten. Når en leser regler om «profilering» må man for eksempel vite at ordet er definert og gitt meningsinnholdet «enhver form for automatisert behandling av personopplysninger som innebærer å bruke personopplysninger for å vurdere visse personlige aspekter knyttet til en fysisk person, særlig for å analysere eller forutsi aspekter som gjelder nevnte fysiske persons arbeidsprestasjoner, økonomiske situasjon, helse, personlige preferanser, interesser, pålitelighet, atferd, plassering eller bevegelser».[6]

Personvernkommisjonen mener norske myndigheter ikke må slå seg til ro med og akseptere en situasjon der det er vanskelig å finne ut av hvilke regler som gjelder og hvordan disse skal

---

2 Se personvernforordningen art. 17 nr. 1.
3 Se personvernforordningen art. 17 nr. 3 bokstav d.
4 Se f.eks. personvernforordningen art. 25 nr. 1.
5 Se f.eks. personvernforordningen art. 22.
6 Se personvernforordningen art. 4 nr. 4.

forstås. Både hensynet til rettsbeskyttelsen av den enkelte, og rettssikkerheten for behandlingsansvarlige og databehandlere tilsier et kontinuerlig arbeid for å gjøre rettsreglene så forståelige som mulig.

I en situasjon med stort behov for europeisk og global regulering av personvern, er det etter *Personvernkommisjonens* syn ikke realistisk å stille krav om en ideell rettslig regulering. De positive virkningene av det europeiske personvernregelverket er langt på vei viktigere enn hvor godt regelverket er utformet og hvor lette reglene er å forstå.

Bedre regelverk på personvernrettens område er i stor grad avhengig av rettslige og politiske prosesser i EU. *Personvernkommisjonen* vil understreke betydningen av at Regjeringen deltar aktivt i disse prosessene.

Personvernkommisjonen anbefaler at det bygges kompetanse innen EU- og EØS-rett i forvaltningen, for å sikre solide prosesser i lovarbeid.

10.3 Behov for å regulere personvern på nasjonalt nivå

I det følgende vil *kommisjonen* begrense seg til å drøfte hva norske myndigheter kan gjøre med virkning for behandling av personopplysninger i Norge. Bakgrunnen for drøftelsen er ønsket om å benytte det nasjonale handlingsrommet som personvernforordningen og EØS-avtalen gir. Formålet er både å legge til rette for lojal etterlevelse av europeisk og annet internasjonalt regelverk, og å imøtekomme særlige norske behov for klarhet og sammenheng i den rettslige reguleringen.

10.3.1 Lovgivningspolitiske utgangspunkter

Personvernforordningen gjelder i utgangspunktet likt, «ord for ord», i alle EØS-land. Fordelen med slike felles regler er blant annet at det kan skape grunnlag for rettsenhet. Dessuten kan de mange aktørene som opptrer på tvers av landegrensene innen EØS, lettere få oversikt over hvilke regler som gjelder. Felles europeiske regler begrenser handlingsrommet for nasjonale lovgivere. Således er det ikke adgang til å gi nasjonale bestemmelser som strider mot forordningen. Fordi forordningens bestemmelser er meget vidtfavnende og har virkning for de aller fleste lov- og samfunnsområder, innebærer dette en betydelig begrensning i nasjonal lovgivningsmyndighet.

Ambisjonen om felles europeiske regler er ikke gjennomført fullt ut i personvernforordningen. I forordningen finnes mer enn 30 bestemmelser som gjelder nasjonal regulering. Flere av disse bestemmelsene har mer enn ett element med slikt innhold, noe som innebærer at antallet mulige nasjonale typer av enkeltbestemmelser overstiger 30. Flere av hjemlene har begrenset betydning. *Personvernkommisjonen* har derfor ikke funnet det hensiktsmessig å drøfte alle hjemlene nærmere, men har valgt ut noen viktige *typer* hjemler og *eksempler* på disse.

Personvernkommisjonen vil understreke at personvernforordningen ikke er til hinder for aktiv utøvelse av norsk lovgivningsmyndighet for å ivareta personvern. *Kommisjonen* vil særlig peke på behovet for norsk lovgivning i situasjoner der:

- personvernforordningen inneholder pålegg om å gi nasjonale regler;
- bestemmelser i personvernforordningen stiller vilkår om nasjonal lovgivning med et visst innhold for at behandling av personopplysninger skal være lovlig; og
- det ellers kan sies å være behov for ytterligere nasjonal lovgivning som bro mellom eksisterende nasjonal lovgivning og personvernforordningen.

Videre er det enkelte saksområder som ikke faller inn under personvernforordningen. Noen av disse saksområdene vil komme inn under annen EU-lovgivning, for eksempel politidirektivet som er omtalt i kapittel 7 om justissektoren. I det følgende forholder *Personvernkommisjonen* seg til personvernforordningen.

Personvernkommisjonen mener Regjeringen må føre en aktiv lovgivningspolitikk for å fremme personvern. Det bør alltid være en ambisjon å bruke det norske, nasjonale handlingsrommet som EØS-lovgivningen gir, både for å *supplere* de europeiske reglene, *støtte opp under* og for å *styrke* gjeldende EØS-lovgivning som norske myndigheter ser som spesielt viktig. Eventuelt bør norske myndigheter vedta *avvikende norske regler* dersom det er adgang og tilstrekkelig grunn til det.

10.3.2 Klarere og mer utfyllende regulering av adgangen til å behandle personopplysninger

Personvernforordningen regulerer ikke bare behandlingsansvarlige, databehandlere, registrerte og tilsynsmyndigheter, den stiller på noen punkter også krav til *nasjonale lovgivere*. Dette gjelder for det første i tilknytning til behandlingsgrunnlag, det vil si krav som må være oppfylt for

at det skal være lovlig å samle inn og behandle opplysninger om enkeltpersoner. Visse krav til behandlingsgrunnlag gjelder alle personopplysninger, og det er disse kravene som er omhandlet i dette avsnittet.[7] Det stilles ytterligere krav for å kunne behandle særlige kategorier personopplysninger, det vil si opplysninger som anses å være spesielt sensitive.[8]

De generelle kravene til regulering av behandlingsgrunnlag i nasjonal lovgivning er særlig knyttet til behandling av opplysninger i regi av offentlige myndigheter. Dette kan for eksempel gjelde lovpålegg om å samle inn og utlevere opplysninger til det offentlige, for eksempel plikt for arbeidsgivere om å rapportere opplysninger til Skatteetaten, Arbeids- og velferdsetaten og Statistisk Sentralbyrå i samsvar med a-opplysningsloven.[9] Personvernforordningen stiller også krav til lovgivning når adgangen til å behandle personopplysninger er begrunnet i at behandlingen er «nødvendig for å utføre en oppgave av allmennhetens interesse», for eksempel dersom det skal gjennomføres undersøkelser av samfunnsforhold og sosiale forhold (trafikkforhold, forurensing, prestasjoner i skolen). Det stilles også krav til nasjonal lovgivning når begrunnelsen for å behandle personopplysninger er at behandlingen er «nødvendig for utøvelse av offentlig myndighet…».[10] Dette gjelder både enkeltvedtak og generelle vedtak (herunder forskrifter), men enkeltvedtak er det mest praktiske.

Når det blir behandlet personopplysninger med henvisning til de nevnte rettslige grunnlagene, fastsetter personvernforordningen at grunnlaget skal «fastsettes i … medlemsstatenes nasjonale rett». Formålet med behandlingen, altså årsaken til at personopplysningene blir behandlet, *skal* i nevnte tilfeller fastsettes i nasjonal rett. I tillegg åpnes det for at en rekke andre spørsmål *kan* undergis nasjonal regulering.[11]

Etterlevelse av skal-kravet er en selvfølge. *Personvernkommisjonen* mener i tillegg norske myndigheter bør benytte anledningen forordningen gir til mer utfyllende regulering. Slik utfyllende regulering kan for eksempel gjelde generelle vilkår for at en bestemt behandling av personopplysninger skal være lovlig, hvilken type opplysninger som kan behandles og hvem personopplysninger kan utleveres til. På den måten kan det utformes bestemmelser som blir mer konkrete enn bestemmelsene i personvernforordningen, og som dermed blir lettere å forstå og etterleve.

I samsvar med norsk rettstradisjon, legger *kommisjonen* til grunn at slike nærmere bestemmelser om behandlingsgrunnlag blir fastsatt i lov og forskrift. Nevnte regler må etter *Personvernkommisjonens* syn ikke bare gis for å kompensere for inngrep i personvernet som lovgiver ønsker å gjøre. *Personvernkommisjonen* mener det er *generelt behov* for å klargjøre det rettslige grunnlaget for behandling av personopplysninger knyttet til offentlig sektor. *Kommisjonen* mener slik rettslig klargjøring er i tråd med grunnleggende rettsstatlige prinsipper, fordi det bidrar til større grad av forutberegnelighet og etterprøvbarhet. Dessuten innebærer en lovregulering at mulige fremtidige ønsker om endret og utvidet adgang til å behandle personopplysninger krever nye politiske vedtak. Dermed blir viktige spørsmål om personvern også del av det politiske, demokratiske meningsskiftet, noe *kommisjonen* ser som en verdi i seg selv.

10.3.3 Klarere og mer utfyllende regulering av adgangen til å behandle særlige kategorier personopplysninger

Det er i utgangspunktet forbudt å behandle særlige kategorier personopplysninger, altså opplysninger som er angitt i personvernforordningen artikkel 9 nr. 1. Slike opplysninger anses generelt å være sensitive. Dette gjelder opplysninger om «rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering». Forbudet er imidlertid mest et regelteknisk utgangspunkt. Det er likevel lov å behandle de nevnte opplysningstypene dersom bestemte vilkår i forordningen er oppfylt. Noen av vilkårene er knyttet til konkrete vurderinger av det enkelte tilfellet. Andre vilkår er av generell karakter og stiller krav til nasjonal lovgivning. Formelt sett er det ikke pålegg i forordningen om å gi nasjonal lovgivning. Siden et velfungerende samfunn er avhengig av å behandle særlige kategorier personopplysningstyper, er det i praksis likevel nød-

7 Se personvernforordningen art. 6 nr. 1.

8 Se personvernforordningen art. 9 nr. 2.

9 Lov 22. juni 2012 nr. 43 om arbeidsgivers innrapportering av ansettelses- og inntektsforhold m.m. (a-opplysningsloven).

10 Begge de sist nevnte situasjonene er regulert i personvernforordningen art. 6 nr. 1 bokstav e.

11 Se personvernforordningen art. 6 nr. 3 bokstav b.

vendig å ha nasjonal lovgivning slik at behandling av nevnte opplysninger i visse tilfeller blir tillatt.

Fem av ti alternativer i artikkel 9 nr. 2 gjør behandling av særlige kategorier personopplysninger lovlig under forutsetning av at visse krav til nasjonal rett er oppfylt. Behovet for nasjonale bestemmelser i tråd med forordningens krav, bør vurderes for disse alternativene:

- behandlingen er nødvendig for å oppfylle forpliktelser og utøve rettigheter på området arbeidsrett, trygderett og sosialrett (jf. bokstav b);
- behandlingen er nødvendig av hensyn til viktige allmenne interesser (jf. bokstav g);
- behandlingen er nødvendig i forbindelse med forebyggende medisin, arbeidsmedisin, medisinsk diagnostikk, og yting av helse- og sosialtjenester og -systemer mv. (jf. bokstav h);
- behandlingen er nødvendig av allmenne folkehelsehensyn eller for å sikre høye kvalitets- og sikkerhetsstandarder for helsetjenester, legemidler og medisinsk utstyr (jf. bokstav i);
- behandlingen er nødvendig for arkivformål i allmennhetens interesse, og formål knyttet til vitenskapelig og historisk forskning og statistiske formål (jf. bokstav j).

I flere av alternativene nevnt ovenfor gjelder også andre, samtidige krav, men her avgrenses det til kravene til nasjonal rett. Det grunnleggende kravet som stilles i nevnte bestemmelser er at spørsmål om behandling av særlige kategorier personopplysninger skal være regulert. I samsvar med norsk rettstradisjon vil regulering i lov og forskrift være de viktigste reguleringsformene. Forordningen nevner imidlertid også tariffavtale (se artikkel 9 nr. 2 bokstav b) og avtale med helsepersonell (se bokstav h).

Opplysninger om blant annet etnisitet, religion, helse og seksuelle forhold er blant de aller mest sensitive personopplysningene, der misbruk lett kan innebære vesentlige krenkelser av den enkeltes personvern.

Når det gjelder behandling av genetiske opplysninger, biometriske opplysninger og helseopplysninger, mener *Personvernkommisjonen* det må vurderes om det skal gis nasjonale regler som opprettholder, eventuelt innfører nye vilkår for behandling av slike opplysninger.[12]

10.3.4 Særlig om lovregulering av helt automatiserte, individuelle avgjørelser

Personvernforordningen artikkel 22 inneholder en rett for den enkelte til ikke å være gjenstand for helt automatiserte avgjørelser med rettslige konsekvenser, eller som på tilsvarende måte påvirker den enkelte, herunder profilering. Slike avgjørelser er aktuelle i både privat og offentlig sektor. Graden av automatisering ved behandling av personopplysninger i det norske samfunnet er økende. Helt automatisert behandling, uten noen form for involvering fra et menneske, blir stadig mer praktisk. Kredittvurdering og e-rekruttering uten menneskelig inngripen er for eksempel ofte helt automatisert, og kun styrt av forhåndsprogrammerte kriterier. Innen offentlig forvaltning er skatteberegning av personlige skattytere ett av flere eksempler på helt automatiserte enkeltvedtak, som beskrevet i kapittel 6.

Bestemmelsen i artikkel 22 er formulert som en rettighet, men har av norske og andre lands myndigheter vært fortolket som et *forbud* mot helt automatisert behandling av personopplysninger. Forordningen åpner uansett for å gi nasjonale regler som tillater slik helt automatisert behandling. I Norge var det våren 2022 gitt minst 16 lov- og forskriftshjemler om dette. Disse var spesielt knyttet til pensjonslovgivning, covid-19-ordninger og utlendingsforvaltningen. I de fleste tilfeller har denne standardformuleringen vært anvendt:

> «[Forvaltningsorgan] kan treffe avgjørelser som utelukkende er basert på automatisert behandling av personopplysninger, herunder personopplysninger som nevnt i personvernforordningen artikkel 9 og 10. Behandlingen må sikre partens krav til forsvarlig saksbehandling og være forenlig med retten til vern av personopplysninger. Avgjørelsen kan ikke bygge på skjønnsmessige vilkår i lov eller forskrift, med mindre avgjørelsen er utvilsom. Den registrerte har rett til manuell overprøving av avgjørelsen.»

De to siste setningene i bestemmelsen sier neppe mer enn det som følger av alminnelige forvaltningsrettslige prinsipper og lovgivning. Formuleringene er derfor kun en påminnelse om vern som parter uansett skal ha, og representerer ikke særlige garantier begrunnet i høy automatiseringsgrad.

For å tillate helt automatiserte avgjørelser, forutsetter personvernforordningen at det er «fastsatt egnede tiltak for å verne den registrertes ret-

[12] Jf. personvernforordningen art. 9 nr. 4 som spesielt åpner for slike nasjonale bestemmelser.

tigheter, friheter og berettigede interesser».[13] Dette må særlig forstås som krav til konkrete tiltak i lov og forskrift. I tilknytning til de nevnte hjemlene i norsk lov er det imidlertid ikke gitt nærmere regler for å sikre folks rettigheter og friheter.

Personvernkommisjonen anser det som nødvendig at man gjør grundige vurderinger ved helt automatiserte avgjørelser.

Etter *Personvernkommisjonens* syn må man gi et spesielt vern for personer som utsettes for automatiserte avgjørelser i tråd med forordningens regler. Aktuelle garantier kan for eksempel være skjerpede krav til begrunnelse for de avgjørelser maskinen genererer. Også dokumentasjon av systemet kan være en hensiktsmessig garanti, eventuelt i kombinasjon med ordninger for manuell vurdering og overprøving av innholdet i selve systemløsningen.

Personvernkommisjonen ser et behov for regler som sikrer tilstrekkelig dokumentasjon og gjennomsiktighet i automatiserte avgjørelsesprosesser. Dokumentasjon er en forutsetning for at den enkelte part, eventuelt med hjelp fra en ideell organisasjon eller advokat, *reelt sett* skal være i stand til å motsi resultater fra automatiserte vedtak og ha grunnlag for å klage på avgjørelsen.

Nasjonale regler om hvem som skal regnes som behandlingsansvarlig

Den behandlingsansvarlige er den virksomhet eller person som bestemmer hva personopplysninger skal brukes til og hvilke hjelpemidler som skal benyttes. Når en legger definisjonen til grunn, vil det i mange tilfeller være tvil om hvem som skal regnes som behandlingsansvarlig. Det gjelder særlig i komplekse organisasjoner, for eksempel i større hierarkier innen stat og kommune og innen konsern med komplekse selskapsstrukturer. I visse tilfeller åpner personvernforordningen imidlertid for at nasjonale myndigheter direkte fastsetter hvem som skal ha behandlingsansvar for konkrete behandlinger, eller de særlige kriteriene for plasseringen av ansvaret, jf. artikkel 4 nr. 7.

Personvernkommisjonen mener det er viktig å unngå tvil om hvem som er ansvarlig for etterlevelse av personvernforordningen og personopplysningsloven. *Kommisjonen* anbefaler at den nasjonale adgangen til å skape klarhet i denne plasseringen av ansvar må brukes aktivt. Når det kan være tvil om hvem som er behandlingsansvarlig, bør en derfor om mulig fastsette bestemmelser om dette i lov eller forskrift, slik forordningen åpner for. I kapittel 6 tar *kommisjonen* til orde for at departementene i større grad bør lov- eller forskriftsfeste ansvarsfordelingen der deling av personopplysninger inngår som en del av et større samarbeid mellom forvaltningsorganer og hvor dette kan medføre alvorlige personvernkonsekvenser.

10.3.5 Ideelle organisasjoners rett til å opptre på vegne av registrerte

Personvernkommisjonen mener det kollektive elementet i arbeidet med personvern bør styrkes og gjøres tydelig. I tillegg til at det må legges til rette for at den enkelte selv kan hevde sin rett og beskytte sine friheter, bør det legges til rette for at enkeltindivider kan organisere seg slik at de i fellesskap kan arbeide for å styrke personvernet.

Personvernforordningen åpner for at ideelle organisasjoner som har som allment formål å fremme personvern, kan opptre etter fullmakt fra registrerte personer.[14] I Norge er det mulig at Elektronisk Forpost Norge (EFN) er et eksempel på en slik organisasjon.[15] Etter gjeldende regler kan slike ideelle organisasjoner blant annet klage til Datatilsynet på registrerte personers vegne, og bringe en sak inn for domstolene. Forordningen åpner dessuten for at ideelle organisasjoner kan opptre på vegne av registrerte personer av *eget initiativ*, uten fullmakt fra de registrerte. En slik selvstendig, aktiv rolle er betinget av at ordningen er fastsatt i nasjonal rett.[16]

Personvernkommisjonen mener Regjeringen bør legge til rette for etablering av ideelle organisasjoner med allmenne formål om å arbeide for personvern. Det er viktig at det gis nasjonale regler som klargjør hvilke krav som gjelder for opprettelse av og arbeidet i slike organisasjoner. Et slikt nasjonalt regelverk bør også klargjøre om, og eventuelt i hvilken grad og på hvilken måte, ideelle organisasjoner kan opptre på vegne av registrerte personer uten deres fullmakt. Dette vil stille spesielt strenge krav til forsvarlig organisering og drift av slike foreninger, noe som vil kreve nærmere rettslig avklaring.

---

[13] Se personvernforordningen art. 22 nr. 2 bokstav b.

[14] Se personvernforordningen art. 80 nr. 1.

[15] Se EFNs vedtekter, § 2 om organisasjonens formål.

[16] Se personvernforordningen art. 80 nr. 1.

10.3.6 Betydningen av tvil og fravær av regler i personvernforordningen

Bestemmelser i personvernforordningen går i tilfelle konflikt foran andre nasjonale bestemmelser.[17] En rekke norske lover gjelder behandling av personopplysninger. Det er da avgjørende at slik norsk lovgivning utformes i harmoni med forordningen. Det kan skape utfordringer når forordningen etterlater tolkningstvil som må løses for å utforme nasjonal lovgivning. Et eksempel er forståelsen av *arkivformål i allmennhetens interesse*. Forståelsen av dette begrepet har avgjørende betydning for om personopplysninger må slettes eller om de kan tas vare på for ettertiden. Spørsmålet ble diskutert av Arkivlovutvalget i NOU 2019: 9. Resultatet var forslag til bestemmelser om personvern på arkivområdet, se §§ 22–25 i forslaget.

En lignende situasjon gjelder spørsmålet om hvordan personvernforordningen skal anvendes på personer under 18 år, altså barn og ungdom. Det er for eksempel uklart i hvilken grad personer under 18 år kan kreve innsyn i egne opplysninger, kreve retting og sletting av opplysninger og for øvrig bruke rettighetene i personvernforordningen kapittel 3. I Ingvild Sciøll Ericsons utredning som ligger ved *Personvernkommisjonens* utredning, drøfter hun disse spørsmålene.[18] Fravær av klare regler på dette området, skaper utilfredsstillende forutberegnelighet for barn, foreldre og behandlingsansvarlige.

Et tredje eksempel gjelder adgangen til å benytte maskinlæring og andre metoder for kunstig intelligens. Om dette er personvernforordningen taus, og spørsmålene er heller ikke avklart i forslaget til forordning om kunstig intelligens. Dette kan skape usikkerhet og frykt for å velge ulovlig praksis. Videre kan dette ha nedkjølende effekt for anvendelse av maskinlæring for å styrke personvernet, eksempelvis for å sikre opplysningskvalitet eller analysere sikkerhetstrusler. *Personvernkommisjonen* viser i denne sammenheng til kapittel 11 om innebygd personvern og andre teknologianvendelser i personvernets tjeneste.

Personvernkommisjonen mener det er meget uheldig når fravær av EU-rettslig regulering skaper rettslig usikkerhet uten at nasjonale regler vedtas for å regulere spørsmålene. Dette gjelder særlig spørsmål med stor betydning for personvern, som i eksemplene ovenfor. Etter *kommisjonens* mening bør Regjeringen føre en aktiv politikk for felles europeiske regler. Når dette ikke er mulig eller realistisk innen rimelig tid, bør Regjeringen fremme forslag til nasjonale bestemmelser. Slike regler bør fortrinnsvis foreslås etter konsultasjon med andre land i EØS.

10.3.7 Tiltak for å forbedre lovtekster uten å gjøre innholdsmessige endringer

Avsnitt 8 i fortalen til personvernforordningen inneholder en retningslinje for utforming av nasjonal lovgivning:

> «Når det i denne forordning fastsettes at det kan innføres presiseringer eller begrensninger av dens regler gjennom medlemsstatenes nasjonale rett, kan medlemsstatene, i den grad det er nødvendig av hensyn til sammenhengen og for å gjøre nasjonale bestemmelser forståelige for de personer de får anvendelse på, innarbeide elementer fra denne forordning i sin nasjonale rett.»

Utgangspunktet er at nasjonal lovgivning ikke skal gjenta forordningens ordlyd, men kun utfylle eller presisere i den grad dette ligger innenfor det nasjonale handlingsrommet som bestemmelsene i forordningen gir. Den siterte retningslinjen innebærer en viss oppmykning av dette, og gir muligheter for å lage broer mellom nasjonal lovgivning på personvernrettens område og personvernforordningen. Dette kan gi bedre språklig og innholdsmessig sammenheng mellom personvernforordningen og norsk, nasjonal lovgivning. Det er trolig mest aktuelt å ta inn legaldefinisjoner fra forordningen i norske lovtekster, slik at forståelsen av bærende begreper fremgår direkte av den nasjonale lovgivningen. Også andre tekstelementer kan være aktuelle å gjenta i norsk lov, for eksempel personvernforordningen artikkel 9 nr. 1 som lister opp hvilke personopplysninger som generelt anses å være spesielt sensitive («særlige kategorier personopplysninger»).

Lov- og forskriftsbestemmelser har som regel innhold med selvstendig rettslig betydning. I tillegg kan en tenke seg bestemmelser som kun har som funksjon å opplyse leseren om viktige aspekter ved regelverket og således bidra til riktig lovforståelse. Slike «informasjonsbestemmelser» kan særlig være nyttig for brukere av lovtekster som ikke har juridisk bakgrunn. Personopplysningsloven av 2000 inneholdt for eksempel en bestem-

---

[17] Personopplysningsloven § 2 (som uttrykker den generelle regelen i EØS-loven § 2).

[18] Ericson, I. S. (2022). *Barns samtykkekompetanse på personvernfeltet.* Utredning for Personvernkommisjonen.

melse i § 8 første ledd om at «Personopplysninger (jf. § 2 nr. 1) kan bare behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling, eller behandlingen er nødvendig for…». Frem til «eller behandlingen er nødvendig for…» innebar denne teksten kun en tydeliggjøring av hvordan de foregående bestemmelsene skulle forstås, og hadde ingen selvstendig rettslig betydning.

Personvernkommisjonen mener at, brukt på forsiktig måte, kan informasjonsbestemmelser i norsk, nasjonal lovgivning, være ett av flere virkemidler for å skape bedre sammenheng mellom personvernforordningen og annet relevant regelverk. Særlig kan det være grunn til å bruke denne metoden innen lovgivning som gjelder individuelle rettigheter og som det derfor er en forutsetning at et stort antall mennesker uten juridisk skolering skal kunne forstå. Fremgangsmåten kan også vurderes i sammenheng med regler som gjelder plikter som et stort antall små og mellomstore virksomheter må kunne etterleve.

10.4 Personvernkommisjonens anbefalinger oppsummert

- *Personvernkommisjonen* mener norske myndigheter ikke bør akseptere en situasjon der det er vanskelig å finne ut av hvilke regler som gjelder og hvordan disse skal forstås. Både hensynet til rettsbeskyttelsen av den enkelte, og rettssikkerheten for behandlingsansvarlige og databehandlere tilsier et kontinuerlig arbeid for å gjøre rettsreglene så forståelige som mulig.
- *Personvernkommisjonen* mener Regjeringen bør delta aktivt i rettslige og politiske prosesser i EU for å arbeide for bedre personvernregelverk.
- *Personvernkommisjonen* anbefaler at det bygges kompetanse innen EU- og EØS-rett i forvaltningen, for å sikre solide prosesser i lovarbeid.
- *Personvernkommisjonen* mener Regjeringen må føre en aktiv lovgivningspolitikk for å fremme personvern. Det bør alltid være en ambisjon å bruke det norske, nasjonale handlingsrommet som EØS-lovgivningen gir, både for å *supplere* de europeiske reglene, *støtte opp under* og for å *styrke* gjeldende EØS-lovgivning som norske myndigheter ser som spesielt viktig. Eventuelt bør norske myndigheter vedta *avvikende norske regler* dersom det er adgang og tilstrekkelig grunn til det.
- *Personvernkommisjonen* mener det er *generelt behov* for å klargjøre det rettslige grunnlaget for behandling av personopplysninger knyttet til offentlig sektor. Rettslig klargjøring er i tråd med grunnleggende rettsstatlige prinsipper, fordi det bidrar til større grad av forutberegnelighet og etterprøvbarhet. Dessuten innebærer en lovregulering at mulige fremtidige ønsker om endret og utvidet adgang til å behandle personopplysninger krever nye politiske vedtak. Dermed blir viktige spørsmål om personvern også del av det politiske, demokratiske meningsskiftet, noe *kommisjonen* ser som en verdi i seg selv.
- *Personvernkommisjonen* mener det må vurderes om det skal gis nasjonale regler som opprettholder, eventuelt innfører nye vilkår for behandling av genetiske, biometriske og helserelaterte opplysninger.
- *Personvernkommisjonen* mener det må gis et spesielt vern for personer som utsettes for helt automatiserte avgjørelser i tråd med forordningens regler. Aktuelle garantier kan for eksempel være skjerpede krav til begrunnelse for de avgjørelser maskinen genererer. Også dokumentasjon av systemet kan være en hensiktsmessig garanti, eventuelt i kombinasjon med ordninger for manuell vurdering og overprøving av innholdet i selve systemløsningen.
- *Personvernkommisjonen* ser et behov for regler som sikrer tilstrekkelig dokumentasjon og gjennomsiktighet i automatiserte avgjørelsesprosesser. Dokumentasjon er en forutsetning for at den enkelte part, eventuelt med hjelp fra ideell organisasjon eller advokat, *reelt sett* skal være i stand til å motsi resultater fra automatiserte vedtak og ha grunnlag for å klage på avgjørelsen.
- *Personvernkommisjonen* anbefaler at den nasjonale adgangen til å skape klarhet i hvem som er ansvarlig for etterlevelse av personvernregelverket, må brukes aktivt. Når det kan være tvil om hvem som er behandlingsansvarlig, bør en derfor om mulig fastsette bestemmelser om dette i lov eller forskrift, slik forordningen åpner for.
- *Personvernkommisjonen* mener Regjeringen bør legge til rette for etablering av ideelle organisasjoner med allmenne formål om å arbeide for personvern. Det er viktig at det gis nasjonale regler som klargjør hvilke krav som gjelder for opprettelse av og arbeidet i slike organisasjoner. Et slikt nasjonalt regelverk bør også klargjøre om, og eventuelt i hvilken grad og på hvilken måte, ideelle organisasjoner kan opp-

tre på vegne av registrerte personer uten deres fullmakt. Dette vil stille spesielt strenge krav til forsvarlig organisering og drift av slike foreninger, noe som vil kreve nærmere rettslig avklaring.

- *Personvernkommisjonen* mener Regjeringen bør føre en aktiv politikk for felles europeiske regler. Når dette ikke er mulig eller realistisk innen rimelig tid, bør Regjeringen fremme forslag til nasjonale bestemmelser. Slike regler bør fortrinnsvis foreslås etter konsultasjon med andre land i EØS.
- *Personvernkommisjonen* mener at, brukt på forsiktig måte, kan informasjonsbestemmelser i norsk, nasjonal lovgivning, være ett av flere virkemidler for å skape bedre sammenheng mellom personvernforordningen og annet relevant regelverk. Særlig kan det være grunn til å bruke denne metoden innen lovgivning som gjelder individuelle rettigheter og som det derfor er en forutsetning at et stort antall mennesker uten juridisk skolering skal kunne forstå. Fremgangsmåten kan også vurderes i sammenheng med regler som gjelder plikter som et stort antall små og mellomstore virksomheter må kunne etterleve.

Kapittel 11
Teknologi i personvernets tjeneste

11.1 Teknologi som problem og løsning

Til grunn for dette kapittelet ligger en forutsetning om at teknologi ikke bare kan anvendes på måter som krenker personvernet, men også kan brukes bevisst for å oppnå et bedre personvern. Teknologiske hjelpemidler kan for eksempel hjelpe folk til både å forstå hvilke rettigheter de har, og hjelpe dem med å bruke dem. En rutine for å gi og trekke tilbake samtykke til å behandle personopplysninger kan sikre at reglene for samtykke blir fulgt, forutsatt at rutinen har et kvalitetssikret innhold som er i samsvar med de rettslige kravene. En innsynsrutine kan på lignende måte legge til rette for at det i praksis blir enklere for registrerte personer å be om å få se hvilke opplysninger en virksomhet har om dem. Samtidig kan rutinen sikre at den som krever innsyn gir de nødvendige opplysningene som viser at den som spør er rett person. *Personvernkommisjonen* mener slike teknologiske muligheter til nå ikke er brukt i tilstrekkelig grad.

11.2 Grunnleggende om personvernteknologi

Tanken om at teknologi kan fremme personvern er ikke ny. I 1980-årene ble begrepet «Privacy Enhancing Technologies» («PETs») lansert for å beskrive slike muligheter. Særlig ble det lagt vekt på teknologi som kunne ivareta hensynet til konfidensialitet og anonymitet. Denne tilnærmingen ble senere videreutviklet, og i siste halvdel av 1990-årene ble den bredere tilnærmingen «Privacy by Design» introdusert. Norsk betegnelse er *innebygd personvern*. Innebygd personvern, slik det ble lansert, bygger på syv prinsipper.[1] Prinsippene gjelder primært utvikling av datasystemer, men er også ment å ha betydning for utforming av organisasjoner og forretningsstrategier.

Boks 11.1 Prinsippene for innebygd personvern

1. Vær i forkant, forebygg fremfor å reparere
2. Gjør personvern til standardinnstilling
3. Bygg personvern inn i designet
4. Skap full funksjonalitet
5. Ivareta informasjonssikkerheten fra start til slutt
6. Vis åpenhet
7. Respekter brukerens personvern

«Privacy by Design» er viktig bakgrunn for artikkel 25 i personvernforordningen. Bestemmelsen stiller krav til «data protection by design and by default» (innebygd personvern og personvern som standardinnstilling).[2] I fortsettelsen bruker *kommisjonen* «innebygd personvern», og lar dette både omfatte «privacy by design» og «data protection by default».

De sju prinsippene for innebygd personvern er ikke del av den rettslige reguleringen av spørsmålet i personvernforordningen artikkel 25, men kan ha indirekte betydning for forståelsen av de rettslige kravene. Artikkel 25 pålegger behandlingsansvarlige plikt til å iverksette tekniske og organisatoriske tiltak for å sikre effektiv gjennomføring av personvernprinsippene og verne rettighetene til de personene det er registrert opplysninger om. Denne bestemmelsen blir nærmere gjennomgått i avsnitt 11.4.2.

Det å bruke digital teknologi på måter som gagner personvernet, kan omfatte mer enn det som er vanlig å betegne som innebygd person-

[1] Cavoukian, A. (2009). *Privacy by Design: The 7 Foundational Principles.*

[2] EUs vektlegging av «data protection by design» innebærer muligens en innsnevring i forhold til «privacy by design», men dette går *kommisjonen* ikke nærmere inn på her.

Boks 11.2 Eksempel 1 på innebygd personvern

NAV hadde utviklet en metode og IT-løsning for å lage syntetiske personopplysninger ved hjelp av maskinlæring. I stedet for reelle opplysninger, er det laget en «kunstig befolkning» med virkelighetstro individer. Dermed trenger ikke NAV å teste IT-systemene sine på opplysninger om virkelige mennesker.[1]

[1] Visma. (u.å.). *Sikre testdata for NAV som ivaretar personvern.*

Boks 11.3 Eksempel 2 på innebygd personvern

Systemet for helseopplysninger i Kjernejournalen understøtter blant annet den enkeltes rett til å bestemme over egne opplysninger og bruken av dem. Den enkelte kan se hvilke helseopplysninger som er registrert om dem og hvem som har hatt tilgang til opplysningene. De kan også regulere hvem som skal ha tilgang til opplysningene.

vern. Ovennevnte bestemmelse om innebygd personvern er bare rettet mot behandlingsansvarlige. *Personvernkommisjonen* bruker også begrepet *personvernteknologi* for generelt å betegne teknologi som er begrunnet i en ambisjon om å ivareta og fremme personvern, uansett hvem som står for utviklingen, hva teknologien gjør, og hvem som er brukere. Begrepet dekker et stort spektrum av teknologi; alt fra beslutningsstøtte, altså systemer som hjelper personer å huske og handle slik personvernregelverket krever, til helt automatiserte rutiner som sikrer etterlevelse av personvernregler i samsvar med forhåndsprogrammerte regler. Automatisk etterlevelse kan for eksempel innebære sletting av opplysninger når det er registrert at et samtykke er trukket tilbake. Personvernteknologi kan være mindre, enkeltstående tiltak (slik som slette-eksempelet), men det kan også være moduler i et IT-system med en rekke sammenhengende funksjoner. I avsnitt 11.4.3 illustreres hvordan flere muligheter for å gi teknologisk støtte til registrerte personer kan kombineres i en «rettighetsplattform».

Alle relevante aktører kan tenkes å ha nytte av personvernteknologi, i det minste som beslutningsstøtte. Dette gjelder for det første sentrale aktører i personvernregelverket som behandlingsansvarlige, registrerte personer, databehandlere og personvernombud. Aktører som sertifiseringsorganer, bransjeorganisasjoner og ideelle organisasjoner kan også ha nytte av teknologisk støtte innen sine arbeidsområder. Videre er teknologisk støtte en forutsetning for at tilsynsmyndigheter kan løse sine oppgaver på effektiv og hensiktsmessig måte.

Aktører kan tenkes å anskaffe personvernteknologi på det kommersielle markedet, men tilbudet av slike produkter er til nå begrenset. Det er også mulig å utvikle personvernteknologi til eget bruk, eventuelt i samarbeid mellom flere, som felles systemkomponent til bruk innen en bransje eller i offentlig sektor. Det er for eksempel mulig å etterleve krav til behandlingsprotokoller (jf. personvernforordningen artikkel 30) og legge til rette for forsvarlig behandling av klager fra registrerte personer (jf. artikkel 12 nr. 2), ved å utvikle felles systemkomponenter som den enkelte behandlingsansvarlige kan tilpasse sine datasystemer.

I tilfeller der behandlingsansvarlige har engasjert en eller flere databehandlere, er det praktisk at databehandleravtalen eller instruksen fra behandlingsansvarlige til databehandler fastsetter at databehandler skal bruke bestemte innebygde løsninger eller annen personvernteknologi.[3] Dette kan for eksempel være tilsvarende løsninger som de behandlingsansvarlige selv bruker, eller ville ha brukt dersom de hadde behandlet personopplysningene selv uten bistand fra databehandler.

Produsenter av programvare har ingen rettslige forpliktelser etter personvernforordningen til å bygge personvern inn i produktene sine. Det er derfor viktig å spørre om produsenter i større grad enn i dag kan påvirkes til å lage løsninger som støtter opp under personvern.

Heller ikke personvernombud,[4] bransjeorganisasjoner, sertifiseringsorganer eller ideelle organisasjoner som arbeider med personvern, har rettslig forpliktelse til å anskaffe og bruke personvernteknologi. Slik teknologibruk vil likevel ofte

[3] Jf. personvernforordningen art. 28.

[4] Det er særlig personvernombud som tilbyr sine tjenester til flere, som kan være i posisjon til å ta selvstendige initiativ til å utvikle personvernteknologi.

være hensiktsmessig. Ideelle organisasjoner kan for eksempel utvikle eller videreformidle verktøy for å hindre sporing av nettaktivitet. For eksempel tilbyr organisasjonen Electronic Frontier Foundation (EFF) verktøyet «Privacy Badger» som er et programvaretillegg til nettleseren som automatisk blokkerer skjult sporing.[5]

Personvernteknologi kan også utvikles av tilsynsmyndigheter, eller etter initiativ fra tilsynsmyndigheter. Dersom Datatilsynet vil øke sannsynligheten for at personvernombudene gjør en best mulig jobb, kan én mulig strategi være at tilsynet selv utvikler, eller ber andre om å utvikle, en systemløsning som hjelper personvernombudene å få oversikt over relevante aktiviteter i organisasjonen. En annen løsning er at Datatilsynet utarbeider en standard, funksjonell kravspesifikasjon for systemer som kommersielle programvareprodusenter kan bruke.

Det må stilles strenge krav til kvaliteten av personvernteknologi. Teknologien må være basert på en riktig forståelse av det aktuelle regelverket. Personvernteknologi må dessuten være forsvarlig og hensiktsmessig å benytte.

Personvernteknologi som behandlingsansvarlige selv bruker eller tilbyr registrerte og databehandlere, kommer inn under behandlingsansvarliges plikt til å sikre at personvernregelverket blir fulgt. Personvernforordningen åpner dessuten opp for sertifisering av behandling av personopplysninger som behandlingsansvarlige og databehandlere gjennomfører, se artikkel 42 og 43. Også for produsenter av personvernteknologi, kan det være behov for en sertifiseringsordning som angir tilstrekkelig kvalitet på slike produkter som tilbys på markedet.

Personvernkommisjonen er kjent med, og anerkjenner, Datatilsynets satsing på innebygd personvern. Av særlig betydning er Datatilsynets veiledere «Innebygd personvern og personvern som standard»[6] og «Programvareutvikling med innebygd personvern».[7] Sist nevnte retter seg primært mot teknologer som deltar i utvikling av programvare som behandler personopplysninger. I tillegg har Datatilsynet siden 2017 arrangert årlig konkurranse om «Innebygd personvern i praksis» der de har kåret beste innebygde løsning blant innsendte kandidater.[8]

Personvernkommisjonen vil understreke at teknologi kan være hensiktsmessig virkemiddel for å bedre personvern for alle aktører og i ulike situasjoner. *Kommisjonen* oppfordrer til et positivt og offensivt syn på teknologi i personvernets tjeneste. Dette betyr ikke at *Personvernkommisjonen* mener alle problemer kan elimineres ved hjelp av teknologiske tiltak. Teknologi kan imidlertid ofte dempe og forbedre situasjoner der det ellers ville oppstått mer alvorlige trusler mot personvernet.

For å oppnå god effekt av selve teknologien, er det etter *Personvernkommisjonens* syn neppe alltid avgjørende at systemløsningene er særlig avanserte. Personvernteknologi kan være alt fra apper på mobilen med begrenset funksjonalitet, til avanserte systemer til bruk for forvaltning av store datamengder i tråd med reglene i personvernregelverket. Slik teknologi kan være integrerte deler av digitale løsninger som brukes til blant annet kommersielle formål eller myndighetsformål, eller enkeltstående løsninger med eneste formål å understøtte personvern. *Kommisjonen* mener det er stort rom for innovasjon med mange ubrukte muligheter på dette feltet.

11.3 Beskyttelse mot å bli registrert eller være registrert

For mange mennesker kan det være viktig å unngå registrering, og dermed unngå at opplysninger om dem blir behandlet av andre. Teknologi som kan gi anonymitet og annen sterk beskyttelse av identiteter (for eksempel ved hjelp av kryptering og pseudonymisering), er eksempler på personvernteknologi ved at den bidrar til å unngå registrering eller reduserer antall datapunkter.[9] Sporingsfri modus i nettlesere og etui for å beskytte mot uberettiget avlesing av digitalt pass eller ID-kort («skimming») er eksempler på enkle antisporingstiltak.

Alle kan ha behov for å skjerme seg. Men varslere, undertrykte og diskriminerte grupper, og personer som blir forfulgt («stalking») har spesielt sterke grunner til å unngå registrering og sporing. Journalister og personer som er kilder for pressen kan også ha sterke grunner til å skjerme seg. På den annen side kan samme teknologiske verktøy brukes til å skjule alvorlige forbrytelser,

---

5 Se Electronic Frontier Foundation (EFF). (u.å.). *Privacy Badger is a browser extension that automatically learns to block invisible trackers.*

6 Datatilsynet. (2022). *Innebygd personvern og personvern som standard.*

7 Datatilsynet. (2019). *Programvareutvikling med innebygd personvern.*

8 Datatilsynet. (2022, 1. mars). *Miniseminar og prisutdeling - Innebygd personvern i praksis 2021.*

9 Electronic FronFoundation (EFF). (2022). *Surveillance self-defence.*

og bruken kan ha til hensikt å skjerme seg mot politi og tilsynsmyndigheter.

Personvernkommisjonen går ikke nærmere inn på en diskusjon om en rett til ikke å være registrert og til redusert deltakelse i det digitale samfunnet. Bruk av teknologi som gir vern mot registrering, vil imidlertid ofte være legitimt.

Lovgivningen skaper plikter og rettigheter, og regulerer blant annet når registrering av personopplysninger er lovlig. Er registrering lovlig, må innbyggerne normalt tåle det, og bruken av verktøy for å skjule identitet og registrering vil i så fall ikke uten videre være legitimt. Hvis en forutsetter lojal regeletterlevelse og effektiv rettshåndhevelse, vil det være mindre behov for den enkelte å selv beskytte seg mot registrering. En slik idealsituasjon er imidlertid åpenbart ikke realistisk.

Personvernkommisjonen mener det alltid vil være behov for at innbyggerne beskytter seg selv mot registrering ved hjelp av teknologi, i tillegg til den beskyttelsen tilsynsmyndigheter og politi kan gi dem. Muligheten for at folk selv kan bruke teknologi for å beskytte seg mot ulovlig eller uønsket behandling, må ikke gjøre at offentlige myndigheter nedprioriterer beskyttelsen av innbyggerne. Realistisk sett vil beskyttelsesbehovet alltid være større enn det myndigheter kan sørge for. Tilsynsmyndigheter bør derfor gi råd til privatpersoner om hvordan de kan innrette seg i størst mulig grad for å beskytte seg selv, herunder gi konkret anvisning på aktuelle verktøy.

11.4 Særskilt om innebygd personvern

11.4.1 Overordnet presentasjon

Personvernforordningens artikkel 25 handler om krav til innebygd personvern og personvern som standardinnstilling. Her velger *Personvernkommisjonen* å konsentrere seg om innebygd personvern, og ser spørsmål om standardinnstillinger som del av det først nevnte elementet. Det grunnleggende poenget med bestemmelsen er at den behandlingsansvarlige skal treffe tiltak for å sikre at personvernprinsippene og øvrige bestemmelser i forordningen – særlig rettighetsbestemmelsene – blir effektivt etterlevet.

Bestemmelsen forutsetter spesielt iverksettelse av tekniske og organisatoriske tiltak. Innbefattet i tekniske tiltak er teknologiske tiltak, typisk utforming og funksjoner i digitale systemer som kan sies å fremme personvern. For eksempel kan en utforme systemrutiner som varsler om at personopplysninger er lagret så lenge at sletting bør vurderes, at det er uoverensstemmelse mellom innholdet av samme opplysning i system A og system B, eller som legger til rette for å kreve retting eller sletting av opplysninger.

En bakenforliggende tanke ved innebygd personvern er at behandlingsansvarlige kan utforme systemløsninger som brukes til å behandle personopplysninger på en måte som gjør at systemet jobber for personvernet. Bestemmelsen forutsetter at det er den behandlingsansvarlige som skal sørge for dette. Imidlertid vil mange behandlingsansvarlige ha begrenset mulighet for å realisere ideen om innbygging, da det ikke er mange behandlingsansvarlige som utvikler systemene sine selv. I stedet kjøper de hyllevare, eller anskaffer kommersielt tilgjengelige systemløsninger som blir tilpasset den behandlingsansvarliges bruk.

Programvareprodusentene som tilbyr datasystemer som utfører behandling av personopplysninger, er som tidligere nevnt ikke omfattet av kravene om innebygd personvern. Om disse har personvernforordningen kun en uttalelse i fortalen, der produsentene henstilles om å bidra til at innbygging kan skje:

> «Ved utvikling, utforming, valg og bruk av programmer, tjenester og produkter som er basert på behandling av personopplysninger, eller når personopplysninger behandles for å oppfylle disses funksjon, bør produsenter av nevnte produkter, tjenester og programmer oppmuntres til å ta hensyn til retten til vern av personopplysninger ved utvikling og utforming av nevnte produkter, tjenester og programmer og, idet det tas behørig hensyn til den tekniske utviklingen, sikre at behandlingsansvarlige og databehandlere kan oppfylle sine forpliktelser med hensyn til vern av personopplysninger.»[10]

Sitatet illustrerer forskjellen mellom tilnærmingen i personvernforordningen og EUs forslag til forordning om kunstig intelligens (AI Act).[11] I forslaget til forordning om kunstig intelligens stiller lovgiver krav til utvalgte *produkter* som gjør bruk av slik teknologi, og krav til blant annet produsenter, i stedet for (bare) krav til de behandlingsansvarlige som *anvender* produktene.

---

[10] Se fortalen til personvernforordningen, avsnitt 78.

[11] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, Brussel, 21. april 2021 COM (2021) 206 final.

Innebygd personvern handler ikke bare om tekniske tiltak og teknologi, men omfatter som nevnt også organisatoriske tiltak. I utgangspunktet kan alle organisatoriske tiltak som gir bidrag til etterlevelse av personvernprinsippene og rettighetsbestemmelser i forordningen være relevante. Det er imidlertid flere bestemmelser i personvernforordningen som krever iverksettelse av tekniske og organisatoriske tiltak.[12]

En systematisk og hensiktsmessig forståelse av bestemmelsen om innebygd personvern i artikkel 25 og andre bestemmelser med nært beslektet innhold, taler for å se organisatoriske tiltak i artikkel 25 i sammenheng med de tekniske tiltakene. For eksempel kan en understøtte dataminimeringsprinsippet ved å ha en maskinell rutine som videreformidler personopplysninger fra ett forvaltningsorgan til et annet på en måte som kun gir tilgang til de opplysninger mottakeren faktisk har rett til å se (teknisk tiltak). Uten et slikt skreddersydd opplegg ville overføringen av opplysninger i stedet kunne skje ved at den som skulle ha opplysninger selv forsynte seg med de opplysninger de mente å ha rett til. En arkitektur som på ekstrem måte bryter med dataminimeringsprinsippet er «*Real time bidding*» (RTB-systemer). Dette er en teknologi der personopplysninger kringkastes til et nettverk av annonsører og andre aktører som selv kan velge hva de skal gjøre med opplysningene.[13]

Teknisk opplegg for dataminimert overføring av opplysninger gir redusert tilgang til personopplysninger for mottakeren. I tillegg kan en la én fast instans i avgiverorganet ha ansvar for all utvikling, bruk og vedlikehold av den tekniske løsningen (organisatoriske tiltak). På den måten kan en både sikre at overføringen skjer innenfor den best mulig tekniske løsningen og i regi av de best kvalifiserte individene.

Tekniske løsninger kan nettopp bli tilfredsstillende fordi løsningene eksisterer innenfor en bestemt organisatorisk ramme, med blant annet avklarte ansvarsforhold. Til sammen kan dette gi informasjonsflyt som gir mottakere av opplysninger det de lovlig har krav på ut ifra rettsgrunnlaget – hverken mer eller mindre. Forskjellen er stor fra løsninger der et stort antall opplysninger er gjort tilgjengelig, og de behandlingsansvarlige selv kan avgjøre hvilke opplysninger de vil behandle.

Som antydet ovenfor er det ikke en skarp grense mellom kravene til «innbygging» i artikkel 25 og andre krav i forordningen til tekniske og organisatoriske tiltak. Dette gjelder særlig forholdet til artikkel 32 om «sikkerhet ved behandlingen», en bestemmelse om informasjonssikkerhet. Systematisk og logisk sett ligger denne bestemmelsen innenfor de forpliktelsene som stilles opp i artikkel 25. Artikkel 25 har imidlertid en videre betydning. Bestemmelsen kan derfor sies *også* å innbefatte kravene i artikkel 32. Dersom en har teknologisk bakgrunn og er vant med tekniske og organisatoriske sikkerhetstiltak, kan det være lett å sette likhetstegn mellom «innebygd sikkerhet» og «innebygd personvern». Slik er det imidlertid ikke. Innebygd personvern må først og fremst anses å handle om andre aspekter ved personvernet enn sikkerhet.

11.4.2 Rettslige krav til innebygd personvern

Personvernforordningen inneholder ingen klare og ufravikelige krav om å bygge personvern inn i tekniske og organisatoriske løsninger. Plikten til innbygging avhenger av en rekke vurderinger som til dels har skjønnsmessig innhold, se teksten i boks 11.4. For det første er plikten basert på resultatene av risikovurderinger, altså av en vurdering av sannsynligheten for at enkeltpersoners rettigheter og friheter skal bli krenket på alvorlige måter. Jo mer sannsynlig en alvorlig krenkelse er, desto større rettslig påtrykk blir det i retning av innebygd personvern.

En rekke andre momenter skal også tas hensyn til; blant annet kostnader, den tekniske utviklingen, hvor mange personopplysninger som blir behandlet, hva opplysningene skal brukes til og hvilke opplysningstyper det er tale om. Behandling av personopplysninger kan som nevnt for eksempel anses å innebære stor risiko fordi det blir planlagt å behandle særlige kategorier (sensitive) personopplysninger til inngripende formål, slik som helseopplysninger for å gjennomføre kontroll. Dersom det samtidig er teknisk enkelt og billig å iverksette tiltak for å bygge personvern inn i systemløsningen, for på den måten å redusere risikoen, vil det foreligge plikt til slik innbygging.

Selv om bestemmelsen er meget vurderingspreget og kan være vanskelig å forstå, vil det i mange tilfeller foreligge plikt til å bygge personvern inn i teknologi og tilknyttet organisering. I mange tilfeller vil det for eksempel trolig være en

---

[12] Dette gjelder særlig artikkel 24 om behandlingsansvarliges ansvar og artikkel 32 om sikkerhet ved behandlingen.

[13] Irish Council for Civil Liberties. (2022). *The Biggest Data Breach. ICCL report on scale of Real-Time Bidding data broadcasts in the U.S. and Europe.*

Boks 11.4 Artikkel 25. Innebygd personvern og personvern som standardinnstilling

Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører, skal den behandlingsansvarlige, både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen, gjennomføre egnede tekniske og organisatoriske tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.

rettslig forpliktelse til å ha en digital innsynsrutine, samtykkerutine, rutine for krav om retting og sletting av opplysninger og annet.

Personvernkommisjonen har ikke gjort undersøkelser av graden av etterlevelse av bestemmelsene om innebygd personvern, men har generelt inntrykk av at bestemmelsen i personvernforordningen artikkel 25 blir utilstrekkelig fulgt og håndhevet. I alle tilfelle kan en ut ifra bestemmelsens ordlyd fastslå at det lett vil oppstå stor usikkerhet om hvordan bestemmelsen skal forstås. For å illustrere poenget har *kommisjonen* satt inn teksten i første avsnitt av artikkel 25 i tekstboks 11.4.[14]

Artikkel 25 er et tydelig eksempel på en bestemmelse som gir stort behov for veiledning, både generelt og konkret, som omtalt i kapittel 13. Dette er en bestemmelse som alle behandlingsansvarlig selv må fortolke og gjøre seg opp en mening om hvordan de vil følge. Konklusjonen kan innebære store investeringer og endrede arbeidsmåter i den behandlingsansvarliges virksomhet. For virksomheter med råd til å kjøpe seg juridisk og teknologisk kompetanse, kan dette være en håndterbar situasjon. For andre, for eksempel små kommuner og små virksomheter med begrensede ressurser, kan forsøket på å avklare betydningen artikkel 25 har for dem være langt vanskeligere å håndtere.

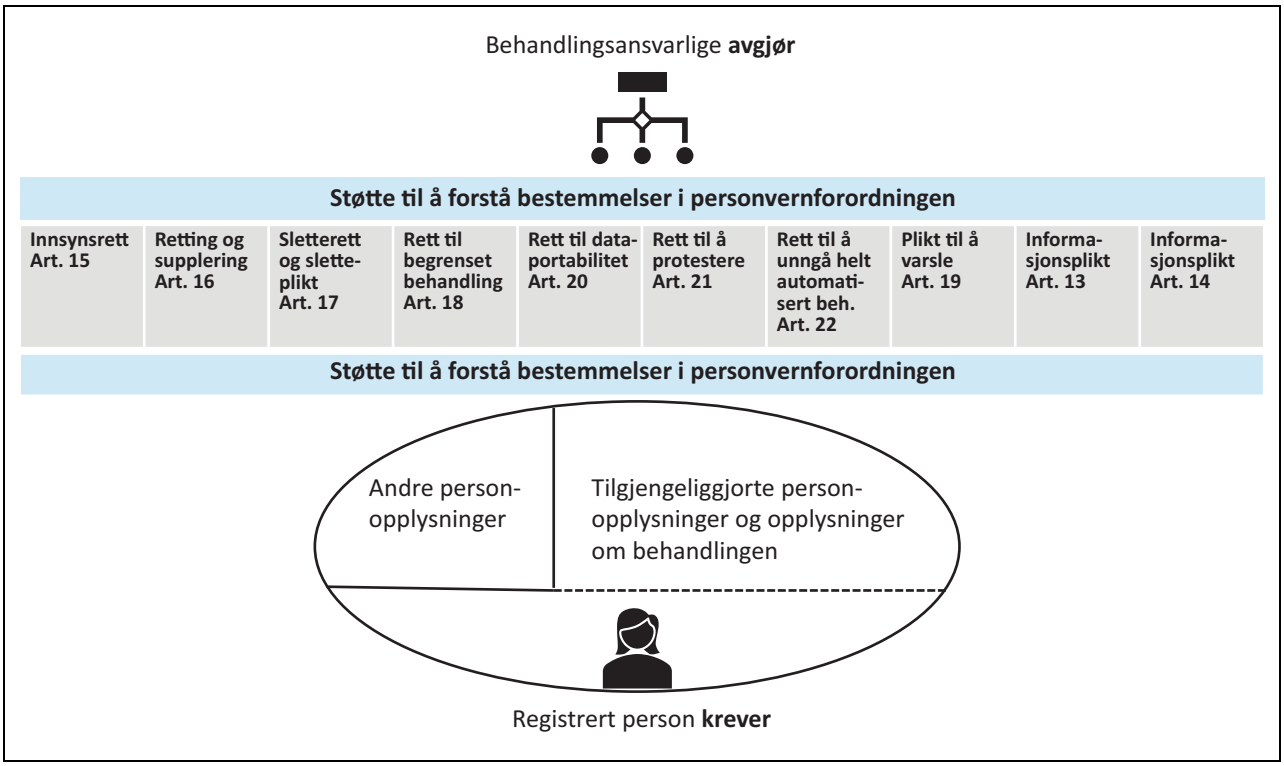
11.4.3 Eksempel på helhetlig innbygging av personvern

I figuren nedenfor blir det illustrert hvordan det kan være mulig å bygge inn bestemmelser som gir registrerte personer rettigheter i en «rettighetsplattform», som er spesielt utformet for å gjøre det enklest mulig for registrerte personer å bruke rettighetene sine. I tråd med det *Personvernkommisjonen* skriver i kapittel 12, er utgangspunktet at registrerte personer kan ha tilgang til de fleste av sine opplysninger uten å måtte kreve innsyn, altså på en slags «min side»-portal. Slik kan personer logge seg inn på en sikker måte og få tilgang til informasjon om seg selv som finnes hos den behandlingsansvarlige. Tilgjengeliggjorte opplysninger kan også omfatte opplysninger om det generelle behandlingsopplegget, jf. artikkel 13 og 14 (om blant annet formål, behandlingsgrunnlag, kilder for og mottakere av personopplysninger). I skissen er muligheten holdt åpen for at enkelte opplysninger ikke er tilgjengeliggjort, men vil kreve begjæring om innsyn (jf. «andre personopplysninger» nederst til venstre i figuren).

Med kunnskap om disse opplysningene kan Rettighetsplattformen også være til hjelp for bruk av andre rettigheter. Registrerte personer kan for eksempel få tilgang til rutiner for å kreve retting, supplering, sletting, begrenset behandling av opplysninger om seg selv – og andre rettigheter slik det fremgår av figuren. Den behandlingsansvarlige må ta stilling til kravene fra de registrerte. Enten blir krav etterkommet eller så nekter den behandlingsansvarlige helt eller delvis å følge den registrertes ønske. Blir det nektet, kan de registrerte bringe uenigheten inn for Datatilsynet for avgjørelse. Datatilsynet kan på sin side ha et digitalt klagesystem som er integrert i og tilgjengelig fra Rettighetsplattformen, som drøftet i kapittel 13.

Plattformen må inneholde veiledende og forklarende tekster som setter de registrerte i stand til å forstå rettighetene sine. De samme eller lignende støttefunksjoner kan være tilgjengelig for behandlingsansvarlige som skal ta stilling til den registrertes krav. Støttefunksjonene vil bidra til å dempe betydningen av at personvernregelverket er komplekst og vanskelig å forstå, som omtalt i avsnitt 10.2.

[14] Bestemmelsen har tre avsnitt.



Figur 11.1 «Rettighetsplattformen»

En rettighetsplattform som skissert kan være en felles komponent for blant annet bransjer, statlig forvaltning og kommunal forvaltning, og kun trenge å tilpasses den enkelte behandlingsansvarlige innen vedkommende bransje, forvaltningsnivå eller lignende. Slik bruk av felles løsninger vil spare utviklingskostnader og gjøre at registrerte personer kjenner seg igjen, uansett bransje eller del av den offentlige forvaltningen.

11.4.4 Personvernkommisjonens vurderinger av innebygd personvern

Personvernkommisjonen mener det bør treffes tiltak for å skape tydeligere plikter til å bygge personvern inn i tekniske og organisatoriske løsninger. *Kommisjonen* er i tvil om i hvilken grad det er adgang til slik klargjøring innenfor rammene av personvernforordningen. Imidlertid mener *kommisjonen* at plikten kan gjøres tydeligere og mer konkret når grunnlaget for behandlingen av personopplysninger er «rettslig forpliktelse», «oppgave i allmennhetens interesse» og «utøve offentlig myndighet», jf. personvernforordningen artikkel 6 nr. 1 bokstavene c og e.

Personvernkommisjonen mener det er viktig å konkretisere plikter til å bygge inn personvern på måter som fremmer åpenhet knyttet til behandling av personopplysninger.

Det er viktig at det offentlige går foran og aktivt bruker personvernteknologi. Derfor mener *Personvernkommisjonen* at bestemmelser som inneholder klare plikter for innebygd personvern bør inngå i ny forvaltningslov. For eksempel bør myndigheter som treffer bebyrdende enkeltvedtak få rettsplikt til å tilgjengeliggjøre personopplysninger for parten, og til å ha en innsynsrutine til bruk for registrerte personer/parter.

Personvernkommisjonen mener det også bør etableres plikt for undervisningsinstitusjoner til å ha innsyns- og informasjonsrutiner til bruk for elever og studenter. *Kommisjonen* viser i denne sammenheng til drøftelsen i kapittel 8 av personvern i skolen og barnehagen. Slike plikter kan for eksempel fastsettes i opplæringslova og universitets- og høgskoleloven.

For forbrukere ønsker *Personvernkommisjonen* å fremheve plikten til å bygge inn bestemmelsene om registrertes rett til å protestere mot direkte markedsføring, jf. personvernforordningen artikkel 21 nr. 2 flg. I artikkel 21 nr. 5 er det gitt en rett for registrerte til å bruke automatiserte midler når slik protest fremsettes i forbindelse med bruk av informasjonssamfunnstjenester.[15] For de som er behandlingsansvarlige for slik direkte markedsføring, gir dette en tilsvarende plikt til å tilby slike automatiserte rutiner. Slik plikt følger direkte av forordningen artikkel

21 nr. 5. De tekniske løsningene skal sikre at protestene automatisk får effekt ved at markedsføringen opphører.

Den rettslige reguleringen pålegger behandlingsansvarlige å bygge personvern inn i teknologi og organiseringen av systemløsningene sine. Det er programvareprodusentene som primært har innflytelse på at slik innbygging faktisk skjer. *Personvernkommisjonen* ser det ikke som hensiktsmessig å stille rettslige krav til norske produsenter av programvare om at programvaren skal understøtte personvern. *Kommisjonen* vil imidlertid peke på muligheten for at offentlig sektor stiller krav om at programvare de gjør bruk av skal tilfredsstille visse standard krav om innebygd personvern. Ved å publisere slike standard krav og la kravene bli et *konkurranseelement ved offentlige anskaffelser*, vil en trolig kunne påvirke kommersiell sektor – både innlands og utenlands.

En standard kravspesifikasjon for personvern i offentlig sektor vil også være til hjelp for ulike behandlingsansvarlige i offentlig sektor, fordi det vil kunne forenkle prosessen med å spesifisere konkrete systemløsninger som skal anskaffes. Standard kravspesifikasjoner er etter hva *kommisjonen* forstår en vanlig og akseptert styringsmåte på IT-området. Således har KS blant annet utformet Nasjonal produktspesifikasjon – Fagsystem for digital byggesaksbehandling (eByggeSak) med siktemål å gi standard krav til digitalisering av byggesaksbehandling i norske kommuner.[16] Også Norsk arkivstandard (NOARK) har i mange år har vært normerende for arkivsystemer i offentlig sektor.[17]

Personvernkommisjonen anbefaler at norske myndigheter stimulerer til utvikling av norsk personvernteknologi. Tiltak kan inkludere blant annet anskaffelseskrav i offentlig sektor, forskningsmidler for å fremme personvernfremmende teknologi, og midler gjennom forskjellige bevilgningsordninger.

11.5 Personvernkommisjonens anbefalinger oppsummert

- *Personvernkommisjonen* mener tilsynsmyndigheter bør gi råd til privatpersoner om hvordan de kan bruke teknologi for å beskytte seg mot ulovlig eller uønsket behandling, herunder gi konkret anvisning på aktuelle verktøy.
- *Personvernkommisjonen* mener det bør treffes tiltak for å skape tydeligere plikter til å bygge personvern inn i tekniske og organisatoriske løsninger. *Kommisjonen* er i tvil om i hvilken grad det er adgang til slik klargjøring innenfor rammene av personvernforordningen. Imidlertid mener *kommisjonen* at plikten kan gjøres tydeligere og mer konkret når grunnlaget for behandlingen av personopplysninger er «rettslig forpliktelse», «oppgave i allmennhetens interesse» og «utøve offentlig myndighet», jf. personvernforordningen artikkel 6 nr. 1 bokstavene c og e.
- *Personvernkommisjonen* mener det er viktig å konkretisere plikter til å bygge inn personvern på måter som fremmer åpenhet om behandling av personopplysninger.
- *Personvernkommisjonen* mener bestemmelser som inneholder klare plikter for innebygd personvern bør inngå i ny forvaltningslov.
- *Personvernkommisjonen* mener det bør etableres plikt for undervisningsinstitusjoner til å ha innsyns- og informasjonsrutiner for elever og studenter. Slike plikter kan for eksempel fastsettes i opplæringslova og universitets- og høgskoleloven.
- *Personvernkommisjonen* anbefaler at norske myndigheter stimulerer til utvikling av norsk personvernteknologi. Tiltak kan inkludere blant annet anskaffelseskrav i offentlig sektor, forskningsmidler for å fremme personvernfremmende teknologi, og midler gjennom forskjellige bevilgningsordninger.

---

15 Informasjonssamfunnstjenester er kommersielle tjenester som leveres elektronisk, på avstand og etter individuell forespørsel. Sosiale medier er et eksempel på informasjonssamfunnstjenester.

16 KS. (u.å.). *Verktøykasse plan- og byggesak.*

17 Arkivverket. (u.å.). *NOARK.*

Kapittel 12
Åpenhet

12.1 Innledning

Åpenhet om hvordan personopplysninger behandles i informasjonssamfunnet er en grunnforutsetning for realisering av viktige idealer i et digitalt moderne demokrati. Derfor mener *Personvernkommisjonen* at åpenhet er en forutsetning for tilfredsstillende demokratisk deltakelse, personvern og rettssikkerhet. Trolig er åpenhet en forutsetning for enhver av de «grunnleggende rettigheter og friheter» som personvernforordningen har som formål å sikre, jf. formålsbestemmelsen i artikkel 1 nr. 2.

Digital teknologi, og særlig internett og sosiale medier, har i stor grad vært anvendt som en åpenhetsteknologi som har gjort det mulig å effektivisere gammeldagse innsynsordninger, tilgjengeliggjøre kolossale mengder informasjon, og gi målrettet informasjon til individer, grupper og allmennheten, for eksempel på bakgrunn av personopplysninger som indikerer informasjonsbehov.

Digital teknologi brukes også for å generere dokumentasjon. For eksempel vil det ofte skje logging av hvordan et datasystem blir anvendt. Slik automatisk generert dokumentasjon og dokumentasjon utformet for å bli brukt av maskiner er for øvrig ikke nødvendigvis egnet som kunnskap for mennesker. Bare de færreste kan nyttiggjøre seg av utskrift av en programkode som styrer distribusjon av personopplysninger og maskinlæringsmodeller som brukes for å profilere enkeltpersoner. Reell åpenhet krever derfor mer enn eksistensen av dokumentasjon og formell tilgang til denne.

Personvernkommisjonen mener at man i et demokrati som respekterer innbyggernes personvern, alltid må kunne forklare resultater som har direkte betydning for innbyggernes plikter, rettigheter, friheter og muligheter. Det er for eksempel ikke tilstrekkelig å kunne observere at noen får banklån og andre ikke, og at noen får 50 dagers samfunnsstraff og andre 30 dagers ubetinget fengselsstraff for tilsynelatende samme lovovertredelse.

Det er også spørsmål knyttet til hvor inngående og detaljert det må være mulig å forklare resultatene. I Norge har vi en solid rettslig forankring for åpenhet og dokumentasjon både som følge av offentleglova og de forvaltningsrettslige prinsippene om begrunnelse, veiledning og innsyn. *Personvernkommisjonen* mener likevel at åpenhet er en så sentral forutsetning at *kommisjonen* understreker at full forklarbarhet må være det klare utgangspunktet, og lavere standarder kun bør aksepteres når effektene antas å være ubetydelige.

På denne bakgrunn mener *Personvernkommisjonen* at myndigheter og andre innflytelsesrike samfunnsaktører kontinuerlig må ha som en av sine viktigste oppgaver å styrke åpenheten knyttet til anvendelser av digital teknologi med direkte betydning for innbyggernes plikter, rettigheter, friheter og muligheter.

Personvernkommisjonen mener de behandlingsansvarlige i langt større grad enn i dag bør tilgjengeliggjøre informasjon knyttet til behandling av personopplysninger. Det bør med andre ord være et mål at registrerte personer og andre interesserte skal kunne skaffe seg tilgang til informasjon uavhengig av andre, ved at informasjonen finnes tilgjengelig på nett, uten at dette krever at den enkelte må be den behandlingsansvarlige om innsyn, eller at den behandlingsansvarlige informerer den enkelte registrerte spesielt. Tilgjengeliggjøring bør være hovedregelen, og innsyn og informering bør være supplerende tilnærminger.

Tilgjengeliggjøring bør som hovedregel både gjelde på individnivå og på kollektivt nivå. Det betyr at enkeltpersoner bør, i så stor grad som personvernforordningen tillater det, ha direkte tilgang til opplysninger om egen person gjennom sikre påloggingsrutiner. Sikring av opplysningenes konfidensialitet, integritet og tilgjengelighet er i denne sammenheng i seg selv en utfordring for personvernet. *Personvernkommisjonen* mener imidlertid at de samme typer sikkerhetstiltak som i dag for eksempel gjelder for innlogging i banktjenester, Altinn og kjernejournal også vil være sik-

kert nok for de aller fleste andre tjenester med tilhørende personopplysninger.

12.2 Forholdet til ytringsfriheten

Personvernkommisjonen ser særlig fire viktige berøringspunkter mellom hensynet til personvern på den ene siden og hensynet til informasjons- og ytringsfrihet på den annen.

- For det *første* vil personvern ofte begrunne begrensninger i bruk og spredning av opplysninger om enkeltmennesker. Særlig når slike begrensninger får anvendelse på personer i mektige posisjoner innen for eksempel politikk, forvaltning, næringsliv og interesseorganisasjoner, vil personvernet kunne begrense mulighetene for å fremføre berettiget kritikk mot enkeltpersoner det er viktig å stille til ansvar.
- For det *andre* kan hets og krasse angrep på personer som ytrer seg i det offentlige rom skape frykt og gi en nedkjølende effekt på lysten til å ytre seg fritt i offentlige rom. Manglende personvern i sosiale medier og andre plattformer som benyttes for å ytre seg, kan *i seg selv* ha en nedkjølende effekt fordi det kan skape en generell usikkerhet om konsekvensene av å ytre seg.
- Et *tredje* berøringspunkt mellom personvern og informasjons- og ytringsfrihet gjelder behovet den enkelte registrerte har for kunnskap om hvordan egne opplysninger blir behandlet. Slik kunnskap kan for eksempel være avgjørende for om personer gir eller trekker tilbake samtykke til å behandle personopplysninger, eller for bruk av de rettigheter som lovgivningen gir.
- For det *fjerde* er det vesentlig at det finnes åpen og offentlig informasjon om hvordan det digitale samfunnet er satt sammen og fungerer. Digital behandling kan bare i meget begrenset grad observeres. Derfor er det av avgjørende betydning at det finnes tilgjengelig informasjon som beskriver det digitale samfunnet, særlig det som direkte gjelder den enkelte innbygger. Dermed begrunner personvern både at det eksisterer informasjon i en form som den enkelte kan tilegne seg, og at det er reell informasjonsfrihet og rett til å bruke denne informasjonen.

I februar 2020 oppnevnte Solberg-regjeringen Ytringsfrihetskommisjonen, som har arbeidet parallelt med *Personvernkommisjonen*.[1] *Personvernkommisjonen* har funnet det mest tjenlig å konsentrere sine diskusjoner av forholdet mellom personvern og informasjons- og ytringsfrihet til spørsmål der det langt på vei kan sies å være *sammenfall* mellom de to grunnleggende rettighetene.

Tilfredsstillende personvern er etter *Personvernkommisjonen*s syn avhengig av både informasjonsfrihet og ytringsfrihet. Her vil *Personvernkommisjonen* legge størst vekt på spørsmål om informasjonsfrihet. Nærmere bestemt vil *kommisjonen* diskutere i hvilken grad og på hvilken måte det er tilstrekkelig åpenhet om den behandlingen av personopplysninger som skjer i samfunnet.

12.3 Nedkjølende effekt av manglende åpenhet

Som beskrevet i kapittel 3, kan nedkjølingseffekter forekomme dersom individer føler at noen «kikker dem over skuldrene». Hvis en føler seg overvåket, vil dette kunne føre til at en endrer oppførsel deretter. Det er problematisk dersom innbyggere vegrer seg fra å ytre seg eller innhente informasjon fordi de er bekymret for at det de gjør registreres og kan brukes mot dem i andre sammenhenger.

I utgangspunktet kan nedkjølingseffekter oppstå uten at det faktisk forekommer overvåkning – så lenge individet tror at de er under overvåkning vil dette kunne føre til endret adferd. Dersom aktører som samler inn og behandler personopplysninger ikke er åpne om hva de samler inn og hva de bruker informasjonen til, vil dette kunne skape usikkerhet og en oppfatning om overvåkning, som kan føre til generell mistillit til aktørene. Åpenhet om behandling av personopplysninger kan dermed være et viktig tillitsbevarende virkemiddel for å motvirke uheldige nedkjølingseffekter.

12.4 Den menneskelige faktoren

Digitaliseringen av samfunnet medfører at behandlingen av personopplysninger i stadig større grad skjer i komplekse digitale økosystem og med stadig større grad av automatisering. Hensynet til bedret konkurransekraft, effektiv tjenesteproduksjon og utøvelse av myndighet er blant argumentene for en slik utvikling. *Personvernkom-*

[1] Kultur- og likestillingsdepartementet. (2020). *Ytringsfrihetskommisjonen.*

misjonen bestrider ikke at dette er gyldige begrunnelser. På den annen side finner *kommisjonen* grunn til å understreke at det også er andre hensyn som bør styre digitaliseringen av samfunnet. Dette gjelder særlig hensynet til innbyggerne.

Ifølge Kompetanse Norge var det i 2020 ca. 600.000 innbyggere som var «ikke-digitale», dvs. ikke deltar aktivt i det digitale samfunnet. Dette gjelder blant annet deler av den eldre befolkningen og unge arbeidsledige:

> «Noen grupper i befolkningen står i større fare enn andre for å bli digitalt utestengt fra samfunnet. Høy alder, lavt utdanningsnivå, lav husholdningsinntekt, mindre sentralt bosted og svak tilknytning til arbeidsmarkedet øker sannsynligheten for å ha svake grunnleggende digitale ferdigheter.»[2]

På den ene side unngår disse personene at det blir registrert visse opplysninger om dem. På den annen side vil de ikke ha tilgang til en rekke tjenester som finnes i digitale kanaler, blant annet hos offentlige myndigheter. Det viktigste er trolig likevel at manglende digital deltakelse lett vil kunne oppleves som utestengelse fra tjenester, beslutningsprosesser og samfunnsarenaer der digitaliseringen har kommet langt. Dette inkluderer også tjenester som skal sikre at innbyggerne skal kunne ivareta sitt personvern.

Det kan diskuteres om *digitalt utenforskap*, som beskrevet ovenfor, bør ses som en del av personvernet. Slikt utenforskap handler ikke primært om person*opplysnings*vern eller privatliv. Spørsmålet gjelder imidlertid muligheten til selvbestemmelse i det digitale samfunnet.

Personvernkommisjonen konstaterer at personvernforordningen artikkel 12 nr. 2 krever at behandlingsansvarlige skal «legge til rette for at den registrerte kan utøve sine rettigheter» etter forordningen. Denne forpliktelsen er ikke begrenset til mennesker som er aktive deltakere i det digitale samfunnet, men gjelder *alle* personer det er registrert personopplysninger om. For den sistnevnte gruppen er de organisatoriske tiltakene trolig viktigst, herunder tiltak som sikrer muligheten for å komme i kontakt med personer som kan gi tilstrekkelig informasjon.

For at det skal være mulig å forstå hvordan behandling av personopplysninger i det digitale samfunnet skjer, er det nødvendig at informasjonen er utformet slik at den som søker informasjonen faktisk er i stand til å tilegne seg denne. Forståelighet handler også om språk. Personvernforordningen artikkel 12 nr. 1 stiller krav om at behandlingsansvarliges kommunikasjon til registrerte personer vedrørende rettigheter skal være «kortfattet, åpen, forståelig og lett tilgjengelig […] og på et klart og enkelt språk». *Personvernkommisjonen* understreker at kravet til klarspråk må gjelde generelt for alle relevante aktører, og for all informasjon som har betydning for ivaretakelsen av folks personvern. Viktig informasjon bør dessuten være tilgjengelig for alle, uansett om de er aktive deltakere i det digitale samfunnet eller ikke.

Det alvorligste problemet vedrørende forståelighet, er trolig muligheten til å forstå *innholdet*. Selv om det eksisterer dokumentasjon skrevet i godt språk betyr det ikke at innholdet automatisk blir forståelig. For de mest avanserte behandlingene av personopplysninger, som for eksempel det som skjer ved bruk av maskinlæring, vil det kreves stor fagkunnskap og arbeidsinnsats for å forstå hvordan behandlingen skjer.

Personvernkommisjonen vil påpeke at samfunnet trolig står ovenfor en situasjon der det blir stadig større strekk i laget, og at mange ikke har tilstrekkelig kunnskap til å forstå de digitale omgivelsene når de blir mer komplekse. Samtidig har mange forutsetninger for å forstå *noe* om hvordan teknologi brukes til å behandle personopplysninger.

12.5 Medvirkning

Lydhørhet handler om at behandlingsansvarlige skal lytte og ta hensyn til registrertes synspunkter og behov, og er i seg selv en form for åpenhet. Samtidig kan lydhørhet bidra til bedre systemer og rutiner som tilfredsstiller flere av de registrertes behov. Etter *Personvernkommisjonens* syn bør lydhørhet i så stor grad som mulig utvikles til å bli reell *medvirkning*. Registrerte personer eller representanter for disse bør aktivt *inviteres* til å delta i prosesser som har direkte betydning for hvordan personopplysninger blir behandlet.

I personvernkonsekvensvurderinger er krav om medvirkning tatt inn. Etter personvernforordningen art. 35 nr. 9 «skal den behandlingsansvarlige innhente synspunkter på den planlagte behandlingen fra de registrerte eller deres representanter». Her er medvirkningsretten betinget av at det er relevant å høre de registrertes syn. *Personvernkommisjonen* antar imidlertid at det ikke kan stilles strenge krav til relevans her, og at medvirkningsretten dermed ofte er relevant.

---

[2] Kompetanse Norge. (2021). *Befolkningens digitale kompetanse og deltakelse*, s. 4

Moderne prinsipper for design, inklusive tjenestedesign, innebærer lydhørhet ovenfor brukerne.[3] Forutsatt at personvern er satt på agendaen som et element som skal ivaretas i den inkluderende prosessen, og at nødvendig kompetanse er til stede, er det etter *Personvernkommisjonens* syn høy grad av sammenfall mellom brukerorienteringen i moderne prinsipper for design og behovet for lydhørhet i utviklingen av løsninger som behandler personopplysninger.

12.6 Åpenhet om håndheving av personvernregelverket

Personvernforordningen gir vid myndighet til Datatilsynet for å håndheve personvernregelverket. Et særpreg ved denne myndigheten er regler som gir adgang til å ilegge meget høye overtredelsesgebyr. De svært høye gebyrnivåene begrunnes blant annet med den avskrekkende effekten dette kan ha.[4] Mulige avskrekkende virkninger forutsetter imidlertid at det faktisk er kjent hvilke gebyrer som ilegges. Hverken i Norge eller i de fleste andre land i EU/EØS finnes det systematiske oversikter som gir informasjon om saker der det er ilagt gebyr og grunnlaget for fastsettelse av størrelsen på gebyret.[5]

Åpenhet rundt håndhevelse er etter *Personvernkommisjonen*s syn viktig av flere grunner. Åpenhet gir samfunnet innsyn og mulighet for kontroll med hvordan tilsynet løser sine kontrolloppgaver, det gir andre behandlingsansvarlige kunnskap om hvordan regelverkets skal forstås, og ikke minst skaper det åpenhet rundt hvordan personopplysninger blir behandlet i ulike virksomheter og de utfordringene dette medfører.

Personvernkommisjonen mener det bør etableres en oversikt over forvaltningsvedtakene knyttet til håndheving av personvernregelverket. Ved etableringen av en slik oversikt bør en vurdere belastningen dette har for kontrollerte virksomheter, og hvordan dette eventuelt kan avhjelpes i formen oversikten etableres, for eksempel gjennom hindre mot indeksering, eller at virksomheters navn i enkelte tilfeller kan utelates i publiserte oversikter. Et slikt behov kan være særlig aktuelt der enkeltvirksomheter kontrolleres som representative i en sektor, og funn kan hefte disproporsjonalt negativt ved virksomheten over tid. Dette må ikke ses som en begrensing av offentligheten i enkeltsakene etter offentleglova.

Personvernkommisjonen mener derfor det bør tilgjengeliggjøres oppdaterte og systematiske fortegnelser med informasjon om i hvilken grad og på hvilken måte Datatilsynet bruker sin myndighet. Dette gjelder enkeltvedtak generelt; særlig saker om irettesettelser (jf. artikkel 58 nr. 2 bokstav b), overtredelsesgebyrer og vedtak om tvangsmulkt. I kapittel 13 diskuterer *Personvernkommisjonen* Datatilsynets myndighetsutøvelser ytterligere og påpeker der også viktigheten av å tilgjengeliggjøre alle høringsuttalelser tilsynet gir på en systematisk og oversiktlig måte.

12.7 Hvordan kan åpenheten bli bedre?

Utgangspunktet for vurderingen av hvordan åpenheten kan bli bedre er at det finnes dokumentasjon av systemene som behandler personopplysninger. Dersom slikt materiale ikke finnes, må det utarbeides i ettertid.

Åpenhet i personvernregelverket er i stor grad basert på informasjon til de registrerte og innsynsrettigheter. *Personvernkommisjonen* mener behandlingsansvarlige i større grad enn i dag bør *tilgjengeliggjøre* informasjon knyttet til behandling av personopplysninger. Det bør være et mål at registrerte personer og andre interesserte skal kunne skaffe seg tilgang til informasjon uavhengig av andre, ved at informasjonen finnes lett tilgjengelig og på en måte som er lett å forstå. *Personvernkommisjonen* mener videre at avanserte behandlinger av personopplysninger bør beskrives lagvis, slik at informasjonen er dekkende for innbyggere med ulik kompetanse og ulik interesse i detaljene i behandlingen.

Med en slik lagdelt informasjon vil den overordnede funksjonelle beskrivelsen være forståelig for de aller fleste. Den vil være *korrekt,* men samtidig representere ufullstendigheter og forenklinger. Jo lenger ned en kommer i lagene, dess mer dekkende og nøyaktig vil beskrivelsene bli. Samtidig vil krav til spesialisert kompetanse øke.

Det er flere offentlige utvalg som har vurdert og foreslått tiltak knyttet til dokumentasjon av behandlingen av personopplysninger. *Personvernkommisjonen* viser i den forbindelse til både Forvaltningslovutvalget[6] og Arkivlovutvalget.[7] Begge utredningene kommer med forslag om nye doku-

---

3 Digitaliseringsdirektoratet (u.å.). *Design.*

4 Dette sies direkte i personvernforordningen art. nr. 1.

5 Lintvedt, M. N. (2022). *Putting a price on data protection infringement, International Data Privacy Law. 12*(1)

6 NOU 2019: 5 *Ny forvaltningslov – Lov om saksbehandlingen i offentlig forvaltning (forvaltningsloven)*.

7 NOU 2019: 9 *Fra kalveskinn til datasjø – Ny lov om samfunnsdokumentasjon og arkiver.*

Boks 12.1 Digitaliseringsdirektoratets utredning av løsninger for å sikre innbyggerne innsyn og kontroll[1]

Innbyggernes behov

Som innbygger ønsker jeg:

1. Oversikt over personopplysningskilder i offentlig sektor, slik at jeg får en bedre forståelse av hvordan det offentlige fungerer og hvilke personopplysninger som kan finnes om meg.
2. Informasjon om hvordan virksomheter behandler personopplysninger, slik at jeg kan ha tillit til dem og hvordan de behandler informasjon om meg.
3. Veiledning for å søke innsyn på en effektiv og god måte.
4. Oversikt over hvor det finnes opplysninger om meg, slik at jeg får økt forståelse for hvordan opplysningene om meg brukes, og kan søke innsyn i det jeg har behov for.
5. Innsyn i egne opplysninger på et hensiktsmessig språk og form, slik at jeg kan forstå min egen situasjon, virksomhetenes bruk av mine personopplysninger og utøve mine øvrige rettigheter slik som retting og sletting.
6. Råderett over egne personopplysninger, slik at jeg kan ta i bruk tjenester jeg har behov for.

Virksomhetenes behov

Behandlingsansvarlige virksomheter ønsker seg:

1. Oversikt over personopplysninger og hvordan de behandles, slik at virksomheten oppfyller innbyggers rettigheter på en måte som ivaretar åpenhet og tillit, og legger til rette for ansvarlig bruk og viderebruk av personopplysninger.
2. Standardisering av krav til systemer, slik at virksomheten enkelt kan gi innsyn etter personvernforordningen.
3. En *beste praksis* for hva man gir innsyn i og hvordan, slik at det blir enklere å gjøre vurderinger rundt innsyn.
4. Verktøy og prosesstøtte for behandling av innsynskrav, slik at virksomheten kan håndtere innsynskravene på en god og strukturert måte.

[1] Digitaliseringsdirektoratet. (2022). *Innsynsløsning – tekniske og juridiske muligheter. En utredning av løsninger for å sikre at innbyggerne får innsyn og kontroll over egne personopplysninger.*

mentasjonsforpliktelser for offentlig sektor. Ingen av forslagene er foreløpig fulgt opp.

Digitaliseringsdirektoratet har utarbeidet en rapport som ble offentliggjort i juni 2022, som svarer på hvordan man kan gi innbyggere oversikt, innsyn og økt råderett over egne personopplysninger. [8] Rapporten er også omtalt i kapittel 6 om personvernet i offentlig forvaltning.

Utredningen identifiserer ti sentrale behov knyttet til innsyn i personopplysninger, både hos den enkelte innbygger og hos offentlige etater, bedrifter og organisasjoner. Utredningen behandler juridiske og teknologiske forutsetninger og foreslår tre sentrale innsatsområder med tilhørende tiltak for videre arbeid.

Personvernkommisjonen mener utredningens forslag til tiltak er så gode, og treffer behovene *kommisjonen* ser så godt, at *kommisjonen* viser til disse i sin helhet (se boks 12.1 og 12.2):

Personvernkommisjonen mener Digitaliseringsdirektoratet sin utredning bør inngå som en viktig del av den nasjonale personvernpolitikken *kommisjonen* har foreslått.

[8] Digitaliseringsdirektoratet. (2022). *Innsynsløsning – tekniske og juridiske muligheter. En utredning av løsninger for å sikre at innbyggerne får innsyn og kontroll over egne personopplysninger.*

Boks 12.2 Digitaliseringsdirektoratets foreslåtte innsatsområder og tiltak

1 – Oversikt over personopplysninger

For at innbyggeren skal kunne kreve innsyn etter personvernfordningen, må man vite hvem man kan henvende seg til, og om hva. Mange etterspør også generell informasjon om hvordan det offentlige behandler og deler personopplysninger, heller enn et konkret innsyn i egne personopplysninger. God oversikt kan derfor bidra til en forståelse som gjør at innsyn ikke alltid er nødvendig. Innsatsområdet handler om å gi innbyggeren kartet over terrenget.

Tiltak: Tilgjengeliggjøre oversikt for innbygger

I henhold til personvernforordningens art. 13 og 14 skal alle virksomheter publisere en oversikt over hvilke kategorier personopplysninger man behandler, som en del av sin personvernerklæring. Men, en innbygger har en relasjon til mange offentlige virksomheter, noen av dem vet man kanskje ikke om en gang. Gjennom å høste og sammenstille hvem som har disse opplysningene, foreslår vi å tilby innbyggerne en felles oversikt.

Tiltak: Definere rammer og verktøy for behandlingsoversikter

For at innbyggerne skal få en oversikt over hvilke virksomheter som behandler personopplysninger om dem, trenger virksomhetene å strukturere og tilgjengeliggjøre informasjon knyttet til personopplysningene de behandler. Vi foreslår derfor å legge til rette for at virksomhetene kan dele strukturert informasjon i en felles behandlingsoversikt.

Oversikten bør som et minimum inkludere behandlingsansvarliges bruk av personopplysninger man er pliktig til å dokumentere i protokoll jf. personvernforordningens art. 30.

2 – Veiledning og innsyn for innbygger

Innsatsområdet «Veiledning og innsyn for innbygger» representerer på mange måter kjernen i denne utredningen. Å søke innsyn etter personopplysningsloven oppleves i dag som tungt for mange innbyggere. Innsiktsarbeidet vårt har vist at hverken innbyggere eller virksomheter alltid har et klart forhold til hvilket regelverk det søkes innsyn etter.

Innbyggerne har i dag en rett til å kreve innsyn i egne personopplysninger etter personvernforordningen artikkel 15, og alle virksomheter plikter å kunne tilby dette til sine brukere. For en bruker kan det likevel være vanskelig å få opp et helthetlig bilde, nettopp fordi disse opplysningene er spredt på tvers av så mange ulike virksomheter.

Tiltak: Utvikle en løsning som gjør det enklere å be om innsyn

For en innbygger er det ikke nødvendigvis gitt hvor man skal henvende seg eller hvilken type innsyn som passer best for situasjonen. Vi foreslår et tiltak for å samle veiledning og muligheten til å be om innsyn på ett sted, og på den måten sette innbyggeren i sentrum.

Tiltak: Stimulere til deling av erfaringer og løsninger

I arbeidet med denne utredningen har vi sett mange eksempler på gode løsninger, veiledning og praksis knyttet til å skape godt personvern. Vi foreslår å stimulere til økt kompetansedeling, erfaringsutveksling og gjenbruk av tekniske løsninger på tvers.

Tiltak: Etablere en standard for innsyn

Virksomheter opplever i dag at de har mange fagsystemer som ikke understøtter personvern generelt og innsynsretten spesielt. Vi foreslår å etablere en standard for hvordan virksomhetenes systemer skal kunne håndtere innsyn.

3 – Kontroll over egne personopplysninger

Dette innsatsområdet skiller seg fra de øvrige innsatsområdene ved at formålet med tiltakene er økt datadeling, ikke kontroll med offentlige virksomheters bruk av personopplysninger. Formålet er snarere å gi den registrerte tilgang til å bruke egne opplysninger, heller enn innsyn i egne opplysninger.

Tiltak: Definere og gi innbygger tilgang til «Mine kjerneopplysninger»

Vi foreslår å definere et sett med kjerneopplysninger som innbygger har ulik grad av råderett over. Det kan for eksempel være førerkort, vitnemål, inntektsopplysninger, kontaktinformasjon, fullmakter og andre sentrale personopplysninger som er nyttige for innbygger i sin hverdag.

Innbyggeren kan for eksempel dele kontonummer og andre kjerneopplysninger gjennom en digital lommebok, for å bedre tjenesteyting fra ulike virksomheter.

12.8 Personvernkommisjonens anbefalinger oppsummert

- *Personvernkommisjonen* mener åpenhet er en så sentral forutsetning at full forklarbarhet må være det klare utgangspunktet, og lavere standarder kun bør aksepteres når effektene antas å være ubetydelige.
- *Personvernkommisjonen* mener offentlige myndigheter og andre innflytelsesrike samfunnsaktører kontinuerlig må ha som en av sine viktigste oppgaver å styrke åpenheten knyttet til anvendelser av digital teknologi med direkte betydning for innbyggernes plikter, rettigheter, friheter og muligheter.
- *Personvernkommisjonen* mener behandlingsansvarlige i større grad enn i dag bør tilgjengeliggjøre informasjon knyttet til behandling av personopplysninger. Det bør være et mål at registrerte personer og andre interesserte skal kunne skaffe seg tilgang til informasjon uavhengig av andre, ved at informasjonen finnes tilgjengelig på nett, uten at dette krever at den enkelte må be den behandlingsansvarlige om innsyn, eller at den behandlingsansvarlige informerer den enkelte registrerte spesielt.
- *Personvernkommisjonen* mener tilgjengeliggjøring som hovedregel bør gjelde både på individnivå og på kollektivt nivå. Enkeltpersoner bør, i så stor grad som personvernforordningen tillater det, ha direkte tilgang til opplysninger om egen person gjennom sikre påloggingsrutiner. Sikring av opplysningenes konfidensialitet, integritet og tilgjengelighet er i denne sammenheng i seg selv en utfordring for personvernet. *Personvernkommisjonen* mener imidlertid at de samme typer sikkerhetstiltak som i dag for eksempel gjelder for innlogging i banktjenester, Altinn og kjernejournal vil være sikkert nok for de aller fleste andre tjenester med tilhørende personopplysninger.
- *Personvernkommisjonen* understreker at krav til klarspråk må gjelde generelt for alle relevante aktører, og for all informasjon som har betydning for ivaretakelsen av folks personvern. Viktig informasjon bør være tilgjengelig for alle, uansett om de er aktive deltakere i det digitale samfunnet.
- *Personvernkommisjonen* mener lydhørhet i så stor grad som mulig bør utvikles til å bli reell *medvirkning*. Med dette mener *kommisjonen* at registrerte personer, eller representanter for disse, aktivt bør *inviteres* til å delta i prosesser som har direkte betydning for hvordan personopplysninger blir behandlet.
- *Personvernkommisjonen* mener det bør etableres en oversikt over forvaltningsvedtakene knyttet til håndheving av personvernregelverket. Ved etableringen av en slik oversikt bør en vurdere belastningen dette har for kontrollerte virksomheter, og hvordan dette eventuelt kan avhjelpes i formen oversikten etableres, for eksempel gjennom hindre mot indeksering, eller at virksomheters navn i enkelte tilfeller kan utelates i publiserte oversikter. Dette må ikke ses som en begrensing av offentligheten i enkeltsakene etter offentleglova.
- *Personvernkommisjonen* mener det bør gjøres tilgjengelig oppdaterte og systematiske fortegnelser med informasjon om i hvilken grad og på hvilken måte Datatilsynet bruker sin myndighet. Dette gjelder enkeltvedtak generelt, overtredelsesgebyrer og vedtak om tvangsmulkt.
- *Personvernkommisjonen* mener behandlingsansvarlige bør *tilgjengeliggjøre* informasjon knyttet til behandling av personopplysninger. Det bør være et mål at registrerte personer og andre interesserte skal kunne skaffe seg tilgang til informasjon uavhengig av andre, ved at informasjonen finnes lett tilgjengelig og på en måte som er lett å forstå. Avanserte behandlinger av personopplysninger bør beskrives lagvis, slik at informasjonen er dekkende for innbyggere med ulik kompetanse og ulik interesse i detaljene i behandlingen.
- *Personvernkommisjonen* mener Digitaliseringsdirektoratet sin utredning treffer svært godt og bør inngå som en viktig del av den nasjonale personvernpolitikken *kommisjonen* har foreslått.

Kapittel 13
Veiledning, tilsyn og klage

13.1 Bakgrunn og premisser

Personvernkommisjonens mandat sier at *kommisjonen* skal «Drøfte andre tema som viser seg særlig relevante for å gi et helhetlig bilde på den samlede situasjonen for personvernet». For å svare ut dette mandatspunktet har *kommisjonen* valgt å se nærmere på myndighetenes veiledning, tilsyn og klagebehandling. Et velfungerende tilsynsorgan er et nødvendig premiss for å sikre innbyggernes personvern.

En kjede av faktorer virker inn på hva slags personvern vi får. Det begynner med bevissthet om personvernet som verdi, og ender med spørsmål om tilsyn, etterlevelse og håndhevelse av rettsregler og andre normer om personvern. En rekke virkemidler kan anvendes for å sikre god etterlevelse. Tidligere i denne utredningen har *Personvernkommisjonen* drøftet og foreslått en rekke tiltak som kan bidra til forbedret etterlevelse innen bestemte problemområder. De viktigste virkemidlene er blant annet utforming av en personvernpolitikk i staten, bruk av bransjenormer, standardisering, sertifisering og bruk av IT-verktøy for å støtte etterlevelse av personvernregelverket. I dette kapitlet blir det rettet oppmerksomhet mot utvalgte spørsmål om rettsregler og myndighetenes veiledning, tilsyn og klagesaksbehandling, noe som i praksis har stor betydning for ivaretakelsen av personvern.

Personvernet er i dag regulert av et omfattende europeisk regelverk der personvernforordningen har sentral betydning. I tillegg kommer en rekke norske, nasjonale lover. I kapittel 10 er det kort beskrevet hvor stort og komplekst dette regelverket er. Forutsetningen for etterlevelse er at de som behandler personopplysninger har tilstrekkelig kunnskap om hvilke regler som gjelder. Dessuten må behandlingsansvarlige ha ferdigheter som gjør at de kan omsette kunnskapen til handling; de må for eksempel forstå hvordan personvernprinsipper kan bygges inn i tekniske løsninger.

Spørsmål om tolkning av regelverket settes ofte på spissen i situasjoner der anvendelse av regelverket også treffer andre fagområder og hensyn. Fagkompetanse på andre områder kan være avgjørende når personvernregelverket skal anvendes. Det kan handle om skole, helse, finans eller ulike digitale tjenester. I noen tilfeller er personvernet i stor grad avhengig av hvordan norske, nasjonale lover skal fortolkes i sammenheng med personvernforordningen. Helseforskningsloven gir for eksempel en rekke bestemmelser som skal beskytte forskningsdeltakernes personvern og fysiske integritet. Da blir kompetanse innen dette regelverket av stor betydning for de samlede juridiske vurderingene. Dessuten foreskriver personvernregelverket ofte helhetlige og skjønnsmessige vurderinger der andre hensyn enn personvernet kan være tungtveiende. Et eksempel på dette er covid-19-pandemien og vurderingen av Smittestopp-appen, der gode vurderinger forutsatte både kompetanse om pandemien, smitteutvikling og -bekjempelse, samt personvernkompetanse.[1]

Personvernregelverket stiller størst krav til de behandlingsansvarlige. Det såkalte ansvarsprinsippet innebærer at de som behandler personopplysninger om andre må kunne påvise at de etterlever reglene i personvernforordningen. De må dessuten ta ansvar ved å treffe slike tiltak som er nødvendige for å sikre at reglene blir fulgt. I mange tilfeller innebærer dette at de må sette seg inn i vanskelige rettsspørsmål, som ofte har usikre konklusjoner.

Det er begrensede muligheter for behandlingsansvarlige til å få bekreftet eller avkreftet at de har forstått regelverket riktig. Noen behandlingsansvarlige kan betale for tjenester fra advokater og konsulenter. Andre kan ikke eller vil ikke gjøre slike investeringer, eller kjenner ikke sine forpliktelser etter loven.

Problemer med etterlevelse av personvernregelverket kan bli forsterket dersom behand-

[1] Juridika Innsikt. (2021, 9. august). *Smittestopp ble smitteflopp. Har personvern overlevd koronakrise?*

lingsansvarlig er en global aktør som, til tross for store ressurser, ikke er tilstrekkelig motivert til å følge europeisk og norsk lovgivning. For enkelte store aktører, kan et stort og komplekst europeisk regelverk kombinert med god tilgang på juridisk ekspertise, gi muligheter for å unnvike de regler som gjelder. Dermed kan også tilsyn og håndhevelse av reglene bli ekstra krevende.

Behandlingsansvarlige er med andre ord ikke én homogen gruppe, men spenner fra globale, mektige aktører til lokale enkeltpersonsforetak. Gruppen omfatter både seriøse virksomheter som legger mye arbeid i god etterlevelse av gjeldende regler, og virksomheter som ikke tillegger personvern stor vekt og gjør lite for å følge regler. Alle er imidlertid omfattet av det samme ansvarsprinsippet, og alle risikerer å måtte betale betydelige gebyrer dersom de bryter reglene.

Det store og komplekse regelverket kan også være et problem for de det er registrert opplysninger om. For det første, mangler de fleste innbyggere tilstrekkelig kunnskap til å kunne slå fast om en praksis er lovlig eller ikke. For det andre, vil mange ikke være klar over hvilke rettigheter de har til å kreve innsyn, retting, sletting, og til å begrense og protestere mot behandlingen av egne opplysninger. Selv om en er klar over rettighetene sine, kan det være vanskelig å vite hvordan en skal gå frem for å bruke rettighetene. Det kan også være vanskelig å vite hva en konkret kan gjøre dersom den behandlingsansvarlige ikke svarer eller ikke vil gjøre slik den registrerte har bedt om.

Nedenfor har *Personvernkommisjonen* særlig valgt å diskutere behovet for veiledning av behandlingsansvarlige, herunder spørsmålet om hvem som bør gi veiledning og på hvilken måte. Formålet er å gjøre situasjonen mer forutberegnelig og sørge for størst mulig grad av rettssikkerhet for behandlingsansvarlige som ønsker å følge personvernregelverket så godt som mulig.

Personvernkommisjonen ser også på situasjonen for registrerte personer og deres mulighet til å få veiledning og ha kunnskap om rettighetene sine. For de fleste innbyggere er rettigheter noe de gjør bruk av i spesielle situasjoner, særlig når det oppstår uenighet med den behandlingsansvarlige. Da er det viktig at registrerte personer vet hvordan de kan bruke rettighetene sine på effektiv måte. Dersom uenigheter mellom registrerte og behandlingsansvarlige ikke blir løst, er det avgjørende at registrerte personer vet hvordan saken kan bli avgjort på balansert måte.

13.2 Datatilsynet – myndighet, oppgaver og organisering

Som norsk nasjonal myndighet etter personopplysningsloven og personvernforordningen, står Datatilsynet sentralt i alle diskusjoner som gjelder forutsetninger for etterlevelse av personvernregelverket. Det er et avgjørende premiss for de følgende drøftelsene at en ikke gjennomfører endringer som på noen måte kan svekke Datatilsynet.

Etter *Personvernkommisjonens* syn er det grunn til å styrke Datatilsynet. *Kommisjonen* legger imidlertid til grunn at de oppgaver som pålegges Datatilsynet er så store at behovene ikke kan bli dekket fullt ut, selv med betydelig styrking av bemanningen i Datatilsynet. Dette gjelder ikke minst behovet for veiledning om forståelsen av personvernregelverket og sammenhengen med norsk, nasjonal lovgivning.

Personvernkommisjonen mener altså at det både er grunn til å styrke Datatilsynet og behov for å styrke arbeidet med personvern hos andre myndigheter og viktige samfunnsaktører. Et annet premiss for den følgende diskusjonen er at det vil kunne oppstå uenigheter om hvordan personvernregelverket skal forstås. Regelverket er i seg selv så komplekst og vanskelig å anvende, at det nødvendigvis vil oppstå berettiget usikkerhet og uenighet som vanskelig kan avklares. Ekspertise innen det sentrale personvernregelverket, gjør ikke at en kan være sikker på hva som kan anses å være riktige og forsvarlige løsninger, uten at det bringes inn for domstolene til endelig avgjørelse.

Datatilsynet er, og bør være, den fremste fagmyndigheten på personvern og personvernregelverket. Selv om Datatilsynets fortolkninger og avveininger mellom motstridende hensyn ofte vil være velbegrunnede og gode, vil det alltid være rom for berettigede og legitime meningsforskjeller. Et overordnet mål må være både å sikre at Datatilsynets avgjørelser er så gode og balanserte som mulig, og samtidig sikre en reell adgang til å overprøve slike avgjørelser i Personvernnemnda, og i ytterste instans ved domstolene.

13.2.1 Myndighet og oppgaver

Datatilsynet ble opprettet i 1980. Fra ikrafttredelsen av personvernforordningen har hjemmelen for Datatilsynets organisering og oppgaver vært å finne i personopplysningsloven (kapittel 6 og 7).

Datatilsynet er et uavhengig forvaltningsorgan, men er administrativt underlagt Kongen og

Kommunal- og distriktsdepartementet (KDD). Kongen og departementet har ingen instruksjons- eller omgjøringsmyndighet når det gjelder enkeltsaker som avgjøres av Datatilsynet.

Datatilsynet fører tilsyn med, og har vedtakskompetanse ved, behandling av personopplysninger som skjer i medhold av personopplysningsloven, politiregisterloven, helseregisterloven, pasientjournalloven, helseforskningsloven og SIS-loven. Forskrifter tilknyttet disse og forskrifter om kameraovervåkning og arbeidsgivers innsyn i elektronisk lagret materiale, er også omfattet av Datatilsynets kompetanse. Vedtak fattet av Datatilsynet med hjemmel i disse lovene kan klages inn for Personvernnemnda. Datatilsynet skal årlig orientere Kongen om sitt virke gjennom en årsmelding.

Bestemmelser om Datatilsynets oppgaver og myndighet finnes i personvernforordningen (artikkel 57 og 58). Artikkel 57 inneholder en ikke uttømmende liste på 22 punkter med tilsynets oppgaver. Sammenfattet består Datatilsynets oppgaver i hovedsak av:

- Saksbehandling av klagesaker
- Tilsyns og kontrollvirksomhet
- Informasjons- og veiledningsvirksomhet
- Aktiv deltagelse i den offentlige debatt om spørsmål knyttet til personvern, blant annet gjennom høringsuttalelser til nye lovforslag og utredningsarbeid
- Faglig virksomhet, herunder samarbeid med andre norske og internasjonale myndigheter

Datatilsynet har etter artikkel 58 flere typer myndighet. Undersøkelsesmyndigheten innebærer blant annet at tilsynet kan pålegge behandlingsansvarlige å fremlegge informasjon, underrette behandlingsansvarlige eller databehandler om påståtte overtredelser, eller få tilgang til all relevant informasjon for å kunne utføre sine oppgaver. Datatilsynet har i tillegg blant annet myndighet til å gi ulike pålegg til behandlingsansvarlige eller databehandler, innføre forbud mot behandling av personopplysninger, pålegge retting eller sletting av personopplysninger eller ilegge overtredelsesgebyrer.

Datatilsynet har myndighet til å godkjenne ulike behandlinger, bindende virksomhetsregler og adferdsnormer. I tillegg har tilsynet en rådgivende myndighet og kan gi råd til behandlingsansvarlige og avgi uttalelser til nasjonale myndigheter, andre institusjoner, samt allmennheten om spørsmål knyttet til vern av personopplysninger.

Datatilsynet har utstrakt kontakt med andre norske myndigheter. Ifølge Datatilsynets årsrapport fra 2021 deltar tilsynet i flere nasjonale fora og har et stort antall kontaktmøter med statlige aktører.[2] Datatilsynet har også avtaler om faglig samarbeid med flere sentrale statlige virksomheter.

13.2.2 Ledelse, budsjett og årsverk

Datatilsynets direktør utnevnes av Kongen for perioder på seks år om gangen. Tilsynet har 72 ansatte, hvorav syv tilhører administrasjonsavdelingen. De resterende er fordelt på fagavdelingene, og har ansvar for de ulike delene av den faglige virksomheten. Datatilsynet har en svært omfattende veiledningsvirksomhet, og har som ledd i denne ansatt 10 studenter i 25 % stillinger for å bemanne den publikumsrettede veiledningstjenesten.

Etter at personvernforordningen ble implementert i 2018 har både saksmengde, budsjett og antall ansatte i Datatilsynet steget kraftig. Fra 40

[2] Datatilsynet. (2022). *Årsrapport for 2021*.

År	Ansatte	Budsjett	Saker tot.	Meldte avvik	Antall vedtak	Saker oversendt til PVN
2016	40 faste stillinger 3 deltidsstillinger gjennom året (2 studenter og 1 læring)	Kr 45 587 000	1 745	206	564	17
2017	40 faste stillinger 3 deltidsstillinger gjennom året	Kr 50 639 000	1 807	349	683	20
2018	41	Kr 54 411 000	2 654	1 275	246	17
2019	45	Kr 57 672 000	3 118	1 893	285	16
2020	58	Kr 66 703 000	3 271	2 008	252	22
2021	72	Kr 67 845 000	3 474	2 255	306	26

faste stillinger i 2017 har staben økt til 72 i 2021. Av disse er 56 stillinger faste. De midlertidige stillingene er prosjektstillinger knyttet til etablering av sandkassen (6 stykker) og studenter (10 stykker) som betjener Datatilsynets veiledningstjeneste. Antallet innmeldte avvik steg fra 349 i 2017 til 1275 i 2018.[3]

13.2.3 Europeisk samarbeid i saksbehandlingen

13.2.3.1 Personvernrådet

Personvernforordningen skal tolkes likt i alle medlemsstatene, noe som nødvendiggjør et forpliktende, internasjonalt samarbeid mellom datatilsynsmyndighetene. Nasjonale datatilsynsmyndigheter har en plikt til å samarbeide og utveksle informasjon med hverandre i grenseoverskridende saker.

Datatilsynet deltar først og fremst i det europeiske databeskyttelsessamarbeidet gjennom Personvernrådet (European Data Protection Board (EDPB)). Personvernrådet er opprettet i medhold av personvernforordningen. Det består av datatilsynsmyndighetene i EØS, samt datatilsynsmyndigheten for EU-organene (European Data Protection Supervisor (EDPS)). Europakommisjonen og EFTAs overvåkingsorgan (ESA) deltar også i møtene med talerett. Siden Norge ikke er et EU-land, har ikke Datatilsynet stemmerett, og tilsynet kan heller ikke stille som leder eller nestleder av Personvernrådet. Ut over dette deltar Datatilsynet i Personvernrådets arbeid uten begrensninger. Rådet har flere oppgaver, blant annet å gi retningslinjer og veiledende uttalelser om hvordan personvernforordningen skal tolkes.

Datatilsynet oppgir på hjemmesiden sin at de har som strategisk målsatsning å påvirke og lede an i utvalgte prosesser i Personvernrådet. Tilsynet deltar derfor aktivt i Personvernrådet og dets ekspertundergrupper.[4] Datatilsynet har for eksempel vært hovedrapportør for Personvernrådets retningslinjer om avtale som behandlingsgrunnlag for online-tjenester og Personvernrådets retningslinjer om innebygd personvern.[5]

13.2.3.2 Samarbeid i saksbehandlingen

For å sikre at personvernreglene tolkes likt, skal datatilsynsmyndighetene i mange sammenhenger samarbeide om å behandle saker som påvirker personvernet i flere EØS-land. Dette kalles samarbeidsmekanismen eller «One Stop Shop»-mekanismen.

Samarbeidsmekanismen sikrer at reglene tolkes likt i EØS. Fordi datatilsynsmyndighetene koordinerer seg imellom, behøver enkeltpersoner og selskaper bare å forholde seg til én tilsynsmyndighet i slike saker. Samtidig gir det Datatilsynet i Norge mulighet til å påvirke andre lands vedtak når behandlingen av personopplysninger i stor grad påvirker personer i Norge. Saksbehandlingstiden er ofte lengre for slike saker siden de krever europeisk koordinering.

For at datatilsynsmyndighetene skal kunne samarbeide i saksbehandlingen, må det aktuelle selskapet som innklages ha en såkalt hovedetablering i EØS, altså en filial, kontor eller liknende som bestemmer over hvordan selskapet behandler personopplysninger i EØS. Dessuten må saken være grenseoverskridende. Hva som er grenseoverskridende er definert i personvernforordningen artikkel 4 nr. 23.

En rekke av de store globale plattformselskapene har sitt europeiske hovedsete i Irland. Dette, kombinert med krevende irske prosessregler, har ført til at mange klagesaker har hopet seg opp hos irske datatilsynsmyndigheter. I tillegg har irske datatilsynsmyndigheter i praksis har fått svært stor makt over håndhevelsen av det europeiske personvernregelverket. Dette har blitt beskrevet som en regulatorisk flaskehals som har forsinket eller hindret håndheving av personvernforordningen mot de største teknologiselskapene.[6]

I forbindelse med diskusjonen rundt og den eventuelle innføringen av Digital Markets Act[7] er det foreslått at tilsyn med de største globale aktørene kan gjøres på et overnasjonalt nivå, drevet frem av Europakommisjonen. Europakommisjonen har allerede lang erfaring med å håndheve konkurransesaker på et overnasjonalt nivå. Forslaget innebærer at *kommisjonen* skal ha myndighet til å bidra til og eventuelt overta tilsynssaker som gjelder de største aktørene.[8] Et slik overna-

---

3 Datatilsynet. (2022). *Årsrapport for 2021*, s. 16

4 Datatilsynet. (2022). *Årsrapport for 2021*.

5 Datatilsynet. (2019, 3. mai). *Det europeiske Personvernrådet (EDPB)*.

6 Irish Council for Civil Liberties. (2021). *Europe's enforcement paralysis. ICCL's 2021 report on the enforcement capacity of data protection authorities.*

7 Se kapittel 9 om forbrukernes personvern.

8 Euractiv. (2021, 5. november). *DSA: enforcement for very large online platforms moves toward EU Commission.*

	2016	2017	2018	2019	2020	2021
Innkomne saker	18	19	20	16	24	22
Avgjorte saker (realitetsbehandlet)	27	19	15	20	17	26
DTs vedtak opprettholdt	16	11	6	14	8	17
DTs vedtak endret eller opphevet	10	7	8	5	8	7
Vedtaksendring i %	40%	37%	53%	25%	47%	27%

sjonalt tilsyn kan være en mulig vei videre for å styrke håndhevingen mot de største selskapene når personvernforordningen skal revideres. Datatilsynet har også tatt til orde for en styrking av rollen til det Europeiske Personvernrådet (EDPB) i enkeltsaker for å få fortgang i spesielle saker.[9]

Personvernkommisjonen anbefaler at regjeringen arbeider for opprettelse av tilsynsmyndigheter på europeisk nivå med myndighet og ansvar for å sørge for effektiv håndhevelse av personvernregelverket overfor de globale plattformaktørene, tilsvarende bestemmelsene som er inntatt i Digital Markets Act.

13.2.4 Personvernnemnda

Personvernnemnda er et uavhengig kollegialt forvaltningsorgan administrativt underlagt Kongen og Kommunal- og distriktsdepartementet (KDD). Nemnda ble etablert 1. januar 2001, med hjemmel i lov om behandling av personopplysninger (14. april 2000 nr. 31) og er, etter ikrafttredelsen av personopplysningsloven 2018, regulert av lov om behandling av personopplysninger 15. juni 2018 nr. 38 (personopplysningsloven) § 22. Personvernnemnda er et særnorsk forvaltningsorgan, og er ikke del av de europeiske tilsynsmyndighetene. Personvernnemnda har sju faste medlemmer som blir oppnevnt for fire år med adgang til gjenoppnevning for ytterligere fire år. Hvert medlem har sin personlige vara. Nemndas medlemmer og deres vararepresentanter er oppnevnt av Kongen.

Nemnda avgjør klager over Datatilsynets vedtak med mindre noe annet er særskilt fastsatt. Nemnda behandler ikke klager over Datatilsynets vedtak i saker som berører behandlingsansvarlige eller registrerte i flere EU-/EØS-land og som skal behandles etter de særlige reglene i personvernforordningen artikkel 60 til 66.

Nemnda treffer sine vedtak ved alminnelig flertall og er beslutningsdyktig når minst fem av nemndas medlemmer eller deres varamedlemmer deltar. Nemndas vedtak er endelige forvaltningsvedtak og kan ikke overprøves gjennom forvaltningsklage. Spørsmål om gyldigheten av Personvernnemndas vedtak kan bringes inn for domstolene, jf. personopplysningsloven § 25 annet ledd. Søksmål rettes mot staten ved Personvernnemnda.

Siden 2018, da det nåværende personvernregelverket trådte i kraft, har Personvernnemnda avgjort 78 saker. Av disse har én sak blitt brakt inn for domstolene (Legelisten[10]), og personvernnemnda er stevnet i mars 2022 i sakene, PVN-2020-16, PVN-2020-17, PVN-2020-18 og PVN-2020-22 (samme saksøker i alle fire sakene).[11]

Personvernkommisjonen mener det bør gjøres jevnlige evalueringer av Personvernnemda. Evalueringene bør se på om nemda utfører sin funksjon på tilstrekkelig vis, og om den er velfungerende.

13.3 Innledende vurderinger av forutsetninger for god etterlevelse av personvernregelverket

Personvernkommisjonen vil understreke at Datatilsynet er gitt et meget viktig og stort arbeids- og myndighetsområde. Personvern er en helt sentral menneskerettighet som settes under press av den teknologiske utviklingen i informasjonssamfunnet. Datatilsynet er således en meget viktig institusjon for beskyttelsen av Norge som demokratisk rettsstat med mennesker som har stor grad av selvbestemmelse og beskyttelse mot manipulering og krenkelse av private forhold. Datatilsynets ansvars- og arbeidsområde dekker nær sagt alle deler av det norske samfunnet. Oppgavene er mangfoldige: Datatilsynet skal informere og veilede, føre tilsyn og slå ned på manglende etterle-

[9] Datatilsynet. (2022, 17. mars). *Høring i EU-parlamentet.*

[10] PVN-2018-14 M, HR-2021-2403-A

[11] Informasjon innhentet fra Personvernnemda på direkte forespørsel.

velse, og de skal være rådgivere for politiske myndigheter i personvernspørsmål.

Selv om Datatilsynet de siste årene har fått styrket sitt budsjett og økt antall ansatte, er tilsynets kapasitet likevel begrenset sett i forhold til ansvar og oppgaver. Det er derfor behov for fortsatt å styrke Datatilsynets kapasitet og ressurser. *Personvernkommisjonen* har imidlertid ikke tilstrekkelige forutsetninger for å ha konkrete oppfatninger om behov og tempo i en fortsatt styrking av Datatilsynets stilling.

Det er et utbredt problem i flere europeiske land at nasjonale datatilsyn mangler ressurser og kompetanse til å gjennomføre teknisk krevende tilsyn. En rapport fra 2021 publisert av den ideelle organisasjonen Irish Council for Civil Liberties viste at selv om budsjettene til datatilsynene i EUs medlemsstater hadde økt ved innføringen av personvernforordningen, har budsjettene sunket i tiden etter.[12] Rapporten viste også at det er begrenset spesialistkompetanse hos tilsynene. For eksempel hadde kun fem av tilsynene mer enn ti teknologer i staben, mens over halvparten hadde fire eller færre. Det norske Datatilsynet har syv teknologer ansatt.

Denne situasjonen skaper store utfordringer for håndheving i saker som krever spesialistkompetanse, og vil kunne føre til at innbyggere ikke får beskyttelsen de har krav på. Behandlingsløp i klagesaker kan ta uforholdsmessig lang tid på grunn av manglende ressurser, som i praksis kan føre til at klager nedprioriteres.

Personvernkommisjonen ser nødvendigheten i at tilsynsmyndigheter kan gjøre egne prioriteringer for å håndtere prinsipielt viktige saker, også i tilfeller hvor vedtak vil ha effekter utenfor Norges grenser. Likevel er det viktig for innbyggernes rettsikkerhet og tillit til myndighetene at klager kan håndteres på en forsvarlig måte.

Samtidig som det er klart behov for å styrke Datatilsynet, er det *Personvernkommisjonens* oppfatning at personvernet ikke bare kan sikres ved en sterk, sentral tilsynsmyndighet. Hovedstrategien for god etterlevelse av personvernregelverket, må være at en gjør bred og kraftfull innsats for å styrke kompetansen om personvern og sikre tilgang til slik kompetanse på alle samfunnsområder. Dette gjelder virksomheter og myndighetsorganer som selv behandler personopplysninger, andre tilsynsorganer med ansvarsområde som direkte har med personopplysninger å gjøre, og generelt i befolkningen.

God etterlevelse av personvernregelverket krever laginnsats der mange samfunnsaktører deltar og hensyntar personvernet som en integrert del av sin virksomhet, med Datatilsynet som lagleder. *Personvernkommisjonen* mener derfor det må skje en samtidig styrking av Datatilsynets og andre viktige samfunnsaktørers forutsetninger for å bidra til et godt personvern.

Boks 13.1 Tekniske løsninger for tilsyn

Tilsyn med komplisert teknologi skaper behov for nye verktøy. For å kunne kontrollere algoritmiske systemer eller gjøre sveipundersøkelser av nettsteder kan det være nødvendig at tilsynsmyndigheter og forskningsmiljøer har tilgang på teknologiske hjelpemidler.

Forskere ved Princeton University har utviklet flere tekniske løsninger for å avdekke problematisk praksis i digitale tjenester i stor skala. Verktøyene inkluderer blant annet systemer for å avdekke sporing i TV-bokser[1] og for å identifisere manipulativt design i nettbutikker.[2] Disse verktøyene er tilgjengelig som åpen kildekode, og kan tilpasses og brukes av alle som har den nødvendige tekniske kompetansen.

[1] Moghaddam, H. M., Acar, G., Burgess, B., Mathur, A., Huang, D. Y., Feamster, N., Felten, E., Mittal, P., Narayanan, A. (2019). *Tracking Ecosystem of Over-the-Top TV Streaming Devices.*

[2] Mathur, A., Acar, G., Friedman, M., Lucherini, L., Mayer, J., Chetty, M., Narayanan, A. (2019). *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites.*

13.3.1 Samarbeid mellom tilsyn

For å sikre ansvarlig ivaretagelse av personvernet, er det avgjørende at relevante tilsynsmyndigheter har god dialog og samarbeid. Saker kan i mange tilfeller overlappe mellom forskjellige tilsyn, og da er det særlig viktig at disse utveksler kompetanse og erfaring.

På europeisk nivå ble initiativet Digital Clearing House lansert i 2016 som en felleseuropeisk møteplass for tilsynsmyndigheter som arbeider innenfor digitalsektoren. Dette initiativet skal legge grunnlaget for bedre og mer konsekvent tilsynsarbeid på tvers av sektorer og landegrenser.

[12] Irish Council for Civil Liberties. (2021). *Europe's enforcement paralysis. ICCL's 2021 report on the enforcement capacity of data protection authorities.*

Norske tilsynsmyndigheter er også en del av dette initiativet.

Tverrsektorielt tilsynssamarbeid er også på agendaen i Norge. I Meld. St. 25 (2018–2019) står det at Solberg-regjeringen ville «etablere eit nasjonalt samarbeidsforum for å styrkje tilsynet på digitalområdet, etter modell av det europeiske Digital Clearinghouse».[13]

Personvernkommisjonen er kjent med at dette samarbeidsforumet er etablert som en del av Forbrukertilsynets samfunnsoppdrag, og inkluderer Forbrukertilsynet, Datatilsynet og Konkurransetilsynet. Samarbeidsforumet skal sikre mest mulig koordinert og effektiv ivaretakelse av personvernet, forbrukervernet og fri konkurranse i den digitale økonomien, gjennom samarbeid, diskusjoner og informasjonsutveksling.

Datatilsynet og Forbrukertilsynet har også sampublisert en veileder for hvordan digitale tjenesteleverandører skal behandle forbrukeres personopplysninger.[14] *Personvernkommisjonen* erfarer at Norge er en foregangsnasjon på dette området, og at samarbeidet blant de norske tilsynene har vært en inspirasjon for tilsyn i andre europeiske land.

I forbindelse med innføringen av forordning for kunstig intelligens vil det komme nye regler for tilsyn med KI-systemer. Det vil innebære at nasjonale tilsynsmyndigheter skal føre tilsyn med maskinlæringssystemer for å blant annet kontrollere at disse opererer i tråd med lovverket. Det er i skrivende stund ikke avklart hvilke sektortilsyn som vil få ansvar for å føre tilsyn med KI-systemer, og hvordan dette vil samspille med Datatilsynets myndighet under personvernforordningen, men det er nærliggende å tro at tilsyn med KI-systemer vil berøre flere sektortilsyn.[15] En slik tilsynsoppgave vil kreve ytterligere samarbeid og spesialkompetanse, da KI-systemer som regel er svært teknisk kompliserte.

Personvernkommisjonen mener det er svært positivt at norske tilsyn samarbeider for å beskytte forbrukernes rettigheter. Dette samarbeidet bør sikres for fremtiden.

Det norske samfunnet trenger teknologer med gode kunnskaper om sikring av personopplysninger og personvernfremmende teknologi, jurister som kjenner personvernregelverket og sammenhengen med nasjonalt regelverk innen blant annet forvaltningsrett, forbrukerrett og skolelovgivning, og ikke minst samfunnsvitere som forstår mekanismene som gir personvernkrenkelser og konsekvensene dette har. Det er behov for både spesialister og personer der kunnskap om personvern er en integrert del av en bredere kompetanse. Med den sentrale rollen personvern har innen et stort antall rettsområder, er det for eksempel overraskende at personvernrett ikke er et obligatorisk fag ved de juridiske utdanningene.

Personvernkommisjonen mener at god etterlevelse av personvernregelverket i stor grad avhenger av at Datatilsynet, andre tilsynsorganer og virksomheter i privat og offentlig sektor som behandler personopplysninger, kan ansette eksperter og andre personer med grunnleggende kompetanse innen personvern. Et generelt høyere kompetansenivå blant behandlingsansvarlige, vil trolig gjøre at flere har forutsetninger for å forstå regelverket, noe som vil lette Datatilsynets arbeid med å sikre etterlevelse.

Personvernkommisjonen mener andre tilsynsmyndigheter med ansvarsområder som har stor og direkte betydning for ivaretakelse av personvern kan spille en større rolle for personvernet enn de gjør i dag. Dette viderefører samarbeidsforhold som allerede er etablert. Alle aktuelle tilsynsmyndigheter har stor belastning, og det er derfor ikke ledig kapasitet som kan flyttes over til arbeid med personvern. Samtidig som økt ressurstilgang for Datatilsynet må prioriteres, vil det derfor være behov for økt ressurstilgang også for enkelte av disse tilsynene. Slike nye personalressurser bør normalt ikke låses til «rene personvernspørsmål», men generelt bidra til å ivareta personvernspørsmål som er en del av vedkommende tilsynsorgans ansvarsområde. For eksempel må Arbeidstilsynet både kunne føre tilsyn med arbeidsgivers kontroll med ansatte etter bestemmelsene i arbeidsmiljøloven, og samtidig anvende de generelle reglene i personvernforordningen som aktualiseres av kontrolltiltaket.

13.4 Spesielt om behov for veiledning

13.4.1 Datatilsynets veiledningsvirksomhet

Datatilsynet driver utstrakt veiledningsvirksomhet, på mange ulike flater og i ulike former, rettet mot både enkeltindividet, virksomheter og andre interesserte. Tilsynet skriver i årsmeldingen for 2020 at de har som strategisk satsing å bidra til økt kunnskap om og interesse for personvern.[16]

---

13 Meld. St. 25 (2018–2019) *Framtidas forbrukar – grøn, smart og digital*, kap 6.8.

14 Datatilsynet & Forbrukertilsynet. (2020). *Digitale tjenester og forbrukeres personopplysninger.*

15 Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, Artikkel 63.

Hjemmesiden er Datatilsynets viktigste verktøy for veiledningsarbeid og kommunikasjon med ulike målgrupper. Tilsynet produserer og publiserer fortløpende veiledning til ulike deler av personvernregelverket for å kunne hjelpe virksomheter med å tolke og bruke regelverket. Tilsynet driver også informasjon og veiledningsarbeid gjennom å være synlige i samfunnsdebatten. I 2020 etablerte de en podcast som tar opp dagsaktuelle personvernproblemstillinger.[17] Tilsynet driver i tillegg utstrakt foredragsvirksomhet.

Datatilsynet har en veiledningstjeneste rettet mot publikum og virksomheter. I løpet av 2021 mottok veiledningstjenesten i overkant av 5 900 henvendelser.[18] Veiledningstjenesten hadde i 2020 opptil ti deltidsansatte studenter. I tillegg til studentene bidrar jurister, teknologer og samfunnsvitere fra fagseksjonene i den daglige veiledningen på telefon. Statistikken viser at nær halvparten av de som tar kontakt med tjenesten er representanter for virksomheter, og nær halvparten er privatpersoner.

13.4.2 Forhåndsdrøftelser

Dersom den behandlingsansvarlige skal gjennomføre behandlinger av personopplysninger som kan medføre høy risiko for de registrertes rettigheter og friheter, må det gjennomføres en vurdering av personvernkonsekvenser (data protection impact assessment).[19] Dersom den behandlingsansvarlige, etter en vurdering av personvernkonsekvenser, kommer frem til at behandlingen vil medføre høy risiko for de registrertes rettigheter og friheter, må det iverksettes tilstrekkelige tiltak for å begrense risikoen til et akseptabelt nivå. I tilfeller der den behandlingsansvarlige ikke klarer å redusere denne risikoen (det vil si at restrisikoen fremdeles er høy), er det krav om *forhåndsdrøftelse* med tilsynsmyndigheten. Forhåndsdrøftelser er i svært liten grad benyttet. Dels kan dette henge sammen med forberedelsene den behandlingsansvarlige må gjøre i tilknytning til forhåndsdrøftelser. Disse forberedelsene er så omfattende at et initiativ typisk vil ha kommet langt når den behandlingsansvarlige er i stand til å redegjøre for de punktene konsultasjonen omfatter. På et slikt sent stadium kan det være vanskelig for den behandlingsansvarlige å tilpasse seg og ta veiledning i betraktning, for eksempel i tilknytning til anskaffelse og utvikling av IT-systemer. Normalt er det mye enklere for en behandlingsansvarlig å ta hensyn til råd gitt i veiledning på et tidlig stadium. Dette tilsier at behandlingsansvarlige bør ha tilgang til veiledning på et tidlig, heller enn et sent, stadium, og gjerne flere ganger, uavhengig av plikten til forhåndsdrøftelse.

13.4.3 Om behovet for veiledning

Personvernregelverket er, som omtalt i kapittel 10, stort og komplisert, med mange vage og skjønnsmessige formuleringer. Reglene må ofte anvendes sammen med andre nasjonale regler, slik at det lett oppstår uklarhet om hva som er riktig samlet forståelse. Dette skaper et sterkt behov for god veiledning for alle som har plikter og rettigheter etter personvernregelverket.

Gjennom innspillsmøter og samtaler med ulike aktører, har *Personvernkommisjonen* erfart at virksomheter som behandler personopplysninger har et stort behov for informasjon og veiledning om personvernregelverket for å kunne forstå og anvende dette.

Behandlingsansvarlige har ansvaret for behandling av personopplysninger. Dette kan for eksempel være en publisist som samler inn data på sine nettsider og bestemmer hvordan disse skal brukes. Som behandlingsansvarlig må selskapet kjenne til hvilke plikter de har etter regelverket. Normalt er behandlingsansvarlige virksomheter, men det kan også være enkeltpersoner. Gruppen er derfor lite homogen og spenner fra enkeltpersonsforetak til store internasjonale konserner. Veiledningsbehovet avhenger av hvilke interne ressurser den behandlingsansvarlige rår over eller kan kjøpe seg tilgang til. For mange virksomheter vil behovet for veiledning være stort, mens andre har tilstrekkelig tilgang på ekspertise.

Databehandlere, virksomheter som behandler personopplysninger etter avtale med behandlingsansvarlige, som for eksempel tilbydere av lagringstjenester, har relativt få plikter etter regelverket. Men med hensyn til de plikter de har, ligner situasjonen den for behandlingsansvarlige. I det følgende vil ikke databehandlers behov for veiledning bli vurdert spesielt.

Behandlingsansvarlige behøver veiledning både i forbindelse med anskaffelse av datasystemer og ved drift og bruk av disse. Spesielt viktig er anskaffelsessituasjonen, fordi uheldige valg av systemer vil kunne føre til anskaffelser og investeringer som det kan være vanskelig eller dyrt å

16 Datatilsynet. (2021). *Årsrapport for 2020.*

17 Datatilsynet. (2020). *Personvernpodden.*

18 Datatilsynet. (2022). *Årsrapport for 2021.*

19 Se personvernforordningen artikkel 35. Bestemmelsen definerer når det er påkrevd å gjøre en vurdering av personvernkonsekvenser, hva den skal inneholde og hvem som skal gjennomføre den.

korrigere senere. Personvernregelverket gjelder ikke direkte for produsenter av programvaren som brukes til å behandle personopplysninger. Behandlingsansvarlige kan derfor ikke stole på at produsentene har tatt hensyn til regelverket, eller at det er hensiktsmessig og mulig å bruke programvaren på en måte som er i tråd med gjeldende rettsregler.

Enkeltindivider har behov for veiledning som er forskjellig fra behandlingsansvarliges og databehandleres behov. Noen vil ønske å sette seg inn i reglene før opplysninger om dem blir registrert. For eksempel kan personer ønske å vite hvilke regler som gjelder for de mange opplysningene som blir samlet inn av en moderne, tilkoblet bil, blant annet hvilke regler som gjelder for lydopptak i bilen, eller for overføring av opplysninger til produsentens hjemland. Andre vil vite hvilke regler som gjelder for bruk av helseopplysninger i forskningsprosjekter, før de eventuelt deltar i et slikt prosjekt.

I andre situasjoner vil registrerte personer ønske å finne ut om det behandlingsansvarlige eller databehandler gjør med opplysningene deres er lovlig eller ikke. De kan for eksempel lure på om bilprodusenten har lov til å ta opptak av lyd uten at det er gitt uttrykkelig samtykke til dette. Tilsvarende vil elever og foreldre kunne ønske å vite om læreren har lov til å pålegge elever å bruke en spesiell sporingsapp.

Enkeltindivider kan også trenge veiledning dersom de ønsker å finne ut hvilke rettigheter de har og hvordan de skal gå frem for å bruke dem. For eksempel kan en person være klar over at barnevernet har opplysninger om tidligere problemer med rus, og lure på om det finnes regler som kan motvirke at disse opplysningene spres til andre. Spørsmålet vil ikke bare være avhengig av det sentrale personvernregelverket, men også av nasjonale regler om blant annet taushetsplikt og opplysningsplikt.

God veiledning betyr ikke det samme som å få sikre svar. Selv om det finnes mange rettsspørsmål vedrørende personvern som er tydelige, er det i en rekke situasjoner umulig å være sikker på hva som er riktig lovforståelse eller forsvarlig utøvelse av skjønn. Derfor kan veiledning både bringe klarhet i hva reglene går ut på, men kan også tydeliggjøre rettslig *usikkerhet*.

For behandlingsansvarlige kan manglende forutberegnelighet gjøre at veiledning uansett er utilstrekkelig. De vil derfor kunne ønske forhåndsuttalelser fra Datatilsynet som gjør dem sikrere på hva Datatilsynets vurdering er. I slike situasjoner kan grensen mellom veiledning og vedtak bli uklar. Utgangspunktet er at den behandlingsansvarlige selv må finne ut av hvilke regler som gjelder, og innrette seg etter dette uten noen forhåndsgodkjenning fra Datatilsynet.

Jo mer Datatilsynet gir veiledning på grunnlag av informasjon om en konkret løsning, desto mer vil veiledningen få preg av en avgjørelse. Når Datatilsynet skal treffe vedtak må det imidlertid opplyse alle relevante saksforhold på grundig måte i henhold til prosedyrereglene for tilsyn. *Personvernkommisjonen* mener det er svært viktig at det etableres tydelige rammer for henholdsvis veiledning og tilsyn.

13.4.4 Forholdet mellom Datatilsynets veiledning og tilsyns-/ kontrollvirksomhet

Datatilsynets oppgaver inkluderer både veiledning og tilsyns-/kontrollvirksomhet. *Personvernkommisjonen* ser, basert på henvendelser som *kommisjonen* har mottatt, at det kan være uheldig at samme organ både skal gi veiledning, fatte avgjørelser, utføre tilsyn og kontrollvirksomhet. Noen virksomheter kan være reserverte når det gjelder å søke veiledning, herunder spesielt ved å gi uttrykk for usikkerhet knyttet til riktig forståelse av personvernregelverket, når de vet at det er det samme organet som senere kan føre tilsyn og eventuelt ilegge sanksjoner. Ut fra innspillene *Personvernkommisjonen* har mottatt, er disse utfordringene større for privat enn for offentlig sektor.

Det har stor verdi å kunne konsultere Datatilsynet for veiledning. I praksis er det imidlertid vanskelig å eliminere eventuelle uheldige sider av dette, da Datatilsynet i henhold til personvernregelverket både skal gi veiledning, fatte avgjørelsen og utføre tilsyn.

Personvernkommisjonen ser at det kan være positivt at Datatilsynet benytter innsikt og kunnskap tilsynet opparbeider seg på tvers av veilednings- og tilsyns-/kontrollvirksomhet. Dette kan bidra til at Datatilsynet både er mer kompetent og arbeider mer effektivt.

Tilsvarende dilemmaer finnes på andre myndighetsområder. Nasjonal Sikkerhetsmyndighet (NSM) har for eksempel valgt å inndele sin virksomhet internt, slik at en avdeling gir veiledning mens en annen avdeling utøver kontroll. En ulempe med dette er at det kan gjøre ressursbruken internt suboptimal. En fordel er at det kan styrke tilliten hos publikum og gjøre det lettere å søke råd og være åpen om eventuell usikkerhet.

Personvernkommisjonen konstaterer at problemstillingene knyttet til Datatilsynets veilednings- og tilsynsfunksjon kan se ganske ulike ut avhengig av hvilket perspektiv man tar. Slik *kommisjonen* ser det, kan det være hensiktsmessig at Datatilsynet organiserer seg slik at en behandlingsansvarlig ikke risikerer å få tilsyn basert på informasjon som stammer fra dialog knyttet til Datatilsynets veiledning av virksomheten.

13.4.5 Regulatoriske sandkasser

Kunstig intelligens (KI), særlig maskinlæring, har fått mye oppmerksomhet de siste årene; ikke minst i tilknytning til profilering.[20] Opprettelse av *regulatoriske sandkasser for kunstig intelligens* er en trend i tiden. Information Commissioner's Office (ICO) i Storbritannia og datatilsynene i Frankrike, Sverige, Estland og Island har slike sandkasser eller planlegger å innføre ordningen. I regjeringens nasjonale strategi for kunstig intelligens, er et av tiltakene å etablere en regulatorisk sandkasse for ansvarlig kunstig intelligens.[21] Som en oppfølging av strategien, har Kommunal- og distriktsdepartementet bevilget midler til en regulatorisk sandkasse i regi av Datatilsynet for årene 2021 og 2022.

Målet med sandkassen er å stimulere til innovasjon og utvikling av etisk og ansvarlig KI, og hjelpe enkeltaktører med å følge regelverket og utvikle personvernvennlige KI-løsninger.[22] Datatilsynet har som mål å bruke eksempler og læring fra de ulike prosjektene til å lage veiledning som kan hjelpe andre å ta i bruk kunstig intelligens på en personvernvennlig måte. Datatilsynet vil bruke KI-sandkassen som en pilot for å vurdere om sandkassemetoden kan være et nyttig virkemiddel på mer permanent basis for å hjelpe virksomheter å operasjonalisere personvernet på en god måte.

Datatilsynets sandkasse har stor pågang av søkere, og fyller behovet for veiledning og hjelp til å fortolke personvernregelverket i møte med nye problemstillinger som bruk av kunstig intelligens reiser. Det er en sentral forutsetning for sandkassen at resultatet av prosessen er veiledning og ikke forhåndsgodkjenning eller vedtak.

Siden sandkassen startet opp i januar 2021 er 12 prosjekter plukket ut for veiledning. Prosjektene tas med etter søknad. Selv om sandkassen legger beslag på relativt mye arbeidskapasitet hos Datatilsynet, er primærfunksjonen bemannet med personer i midlertidige stillinger som betales av øremerkede midler.

Datatilsynets sandkasse er, etter hva *Personvernkommisjonen* kan forstå, annerledes enn «AI regulatory sandboxes» som er beskrevet i artikkel 53 i forslaget til forordning om kunstig intelligens. Regulatoriske sandkasser for KI skal ifølge forslaget til forordning være et kontrollert miljø som skal legge til rette for utvikling, testing og validering av KI-systemer. Tilbudet skal være tidsbegrenset, og er aktuelt forut for planlagt lansering av KI-systemer. Slike KI-systemer vil ofte, men ikke alltid, behandle personopplysninger. Uansett vil effektene ikke bare ha betydning for personvern, men også blant annet for diskrimineringsvern og ytringsfrihet. Slike sandkasser vil med andre ord i stor grad gjelde Datatilsynets arbeidsområde, men vil også ha klar relevans for andre myndigheter.

Forslaget til forordning fastsetter at sandkassene ikke skal virke inn på den aktuelle myndighetens tilsynsvirksomhet og myndighet til å kreve endring av løsningene. Det er altså foreslått et klart skille mellom utvikling, testing og validering på den ene side, og myndighetsutøvelse på den annen side.

Formelt treffes det ikke avgjørelser i Datatilsynets sandkasse. Rapportene som gjelder hvert enkelt prosjekt kan likevel reelt sett fungere som forhåndsavgjørelser med prinsipiell betydning. I rapporten om NAVs prosjekt om bruk av maskinlæring for å forutse hvilke sykmeldte brukere som vil ha behov for oppfølging to måneder frem i tid, tar en for eksempel stilling til vanskelige rettsspørsmål uten motstemmer, og uten formell mulighet for å klage konklusjonene inn for Personvernnemnda.

Personvernkommisjonen mener det er positivt at produsenter og distributører av KI-systemer som behandler personopplysninger har tilgang til et forum med mulighet til å diskutere utvikling, testing og validering av KI-løsninger. *Kommisjonen ser* det ikke som et problem at en foreløpig nasjonal ordning med regulatoriske sandkasser legger særlig vekt på personvern. Når forordning for kunstig intelligens tas inn i EØS-avtalen, vil det imidlertid være nødvendig også å vurdere andre aspekter ved slike systemer, spesielt andre frihe-

---

[20] Se kapittel 6 i Lintvedts utredning for *Personvernkommisjonen* av spørsmål knyttet til profilering i offentlig forvaltning. Lintvedt, M. N. (2022). *Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering. Utredning på oppdrag fra Personvernkommisjonen.*

[21] Kommunal- og moderniseringsdepartementet. (2020). *Nasjonal strategi for kunstig intelligens.*

[22] Datatilsynet. (2022). *Sandkassesiden.*

ter og rettigheter som er nært knyttet til personvernet.

Personvernkommisjonen vil bemerke at en ordning med regulatorisk sandkasse innebærer at noen få virksomheter får tilgang til Datatilsynets ekspertise som andre ikke får del i, annet enn gjennom sluttrapportene fra hvert prosjekt. Deltakerne i sandkassen trenger ikke være behandlingsansvarlige, men kan for eksempel være fremtidige produsenter og tilbydere av tjenester. Slike aktører er ikke omfattet av personvernregelverket (men vil komme inn under forordning for kunstig intelligens). Ordningen reiser etter *Personvernkommisjonens* syn noen prinsipielle spørsmål om hvordan begrensede ressurser til tidlig veiledning av behandlingsansvarlige skal fordeles. Selv om tiltaket finansieres av øremerkede midler, bør allokering og prioritering av ressurser til veiledning skje etter en samlet vurdering av hva som gir størst effekt for ivaretakelsen av personvernet.

I en senere ordning med regulatorisk sandkasse for KI i samsvar med forordning for kunstig intelligens, vil hensyn og prioriteringer være annerledes enn i dagens ordning. For eksempel skal en da også vektlegge et bredere spektrum av friheter og rettigheter. I tillegg vil en kunne legge vekt på innovasjon og næringspolitikk. Blant annet vil en kunne prioritere tilbud til små og mellomstore bedrifter, herunder oppstartsbedrifter.

Personvernkommisjonen har ikke noen nærmere oppfatning om hvordan en norsk sandkasse i samsvar med forordning for kunstig intelligens bør organiseres.

Personvernkommisjonen mener at dersom Datatilsynets sandkasse skal videreføres, bør spørsmålene som en tar stilling til i hvert prosjekt legges åpent frem for mulige merknader før konklusjonene treffes. I konklusjonene bør en i tillegg legge stor vekt på å få frem forutsetninger og eventuell tvil knyttet til konklusjonene. Generelt bør rapportene legges opp slik at de i minst mulig grad blir oppfattet som forhåndsavgjørelser.

13.4.6 Behov for veiledning fra andre myndigheter

Behandling av personopplysninger skjer i alle samfunnssektorer. Personvernregelverket har derfor et meget bredt virkeområde, og Datatilsynets arbeidsområde er tilsvarende vidt. Samtidig er det en rekke statlige myndigheter som er tilsyn eller har tilsynsfunksjoner på samfunnsområder der personopplysninger spiller en stor rolle. Arbeidstilsynet, Forbrukertilsynet og Nasjonal kommunikasjonsmyndighet er eksempler på sektortilsyn. Slike tilsyn har det til felles med Datatilsynet at tilsynsoppgavene er knyttet til ivaretakelse av den enkeltes friheter og rettigheter, for eksempel sikre forsvarlig arbeidsmiljø, helsevern, forbrukervern, vern av elektronisk kommunikasjon, og vern av dokumentasjon, herunder personopplysninger. En rekke ulike hensyn på de aktuelle områdene kan stå i et komplekst forhold til det personvernet som Datatilsynet er satt til å ivareta.

I noen tilfeller er det stor grad av sammenfall mellom verneinteressene. For eksempel vil det være delvis sammenfall mellom personvern på den ene siden, og vern mot overdreven overvåking av arbeidstakere, vern mot informasjonskapsler (cookies), sikker lagring av helseopplysninger og arkivalia, på den annen side. I andre tilfeller er det motstrid mellom personvern og annet vern av individet; for eksempel kan hensynet til arbeidsmiljø, helsehjelp og effektive kommunikasjonstjenester, begrunne mer omfattende og langvarig lagring av personopplysninger enn det som vil være ønskelig dersom det kun tas hensyn til personvern.

Datatilsynet er spesialisert på personvern. Retten til vern av personopplysninger er ikke en absolutt rettighet. Derfor skal Datatilsynet også ta hensyn til andre grunnleggende rettigheter og friheter. Flere slike rettigheter og friheter hører til andre tilsynsmyndigheters arbeidsområde, for eksempel «tanke-, tros- og religionsfrihet, ytrings- og informasjonsfrihet, frihet til å drive næringsvirksomhet, retten til effektiv prøving og rettferdig rettergang».[23] Dette fremgår blant annet av formålsbestemmelsen i personvernforordningen.

Datatilsynet har i dag samarbeid med en rekke andre offentlige tilsyn. *Personvernkommisjonen* ser positivt på slikt samarbeid. Denne typen samarbeid er blant annet verdifullt fordi tilsynsvirksomheten kan bli mer effektiv når tilsynene er enige. I tillegg er det etter *Personvernkommisjonens* syn stor verdi i at ulike tilsynsmyndigheter utveksler synspunkter om ulike aspekter ved vern av individet. En slik dialog vil etter *Personvernkommisjonens* syn gjensidig kunne styrke kunnskapen og bevisstheten om de mange komplekse avveiningene som er knyttet til behandling av personopplysninger innenfor eksempel helsevern og arbeidstakervern.

Andre myndigheter har særlig fagkompetanse på sine områder, men har i varierende grad kompetanse innen personvernrett. Etter *Personvernkommisjonens* syn, er behandling av person-

[23] Personvernforordningen fortalepunkt 4

opplysninger en så integrert del av flere andre tilsynsoppgaver, at det ikke kan konstrueres noe klart skille mellom tilsynet med etterlevelsen av sektorregelverket og det generelle personvernregelverket.

Arbeidsgivers kontrolltiltak vil for eksempel innebære behandling av personopplysninger som gjør at hele personvernforordningen kommer til anvendelse samtidig med bestemmelsene om kontrolltiltak i arbeidsmiljøloven. Det vil da være paradoksalt om Arbeidstilsynet kun skal gi veiledning om særlige bestemmelsene i «sin lov» (arbeidsmiljøloven), samtidig som de ikke gir veiledning om andre personvernspørsmål som er del av ett og samme problemkompleks. Et kontrolltiltak kan for eksempel være lovlig ut fra arbeidsmiljølovens bestemmelser fordi tiltaket er saklig begrunnet og ikke gir uforholdsmessig belastning på arbeidstakerne, men likevel være klart ulovlig fordi kontrolltiltaket mangler behandlingsgrunnlag og bryter med formålsbestemthetsprinsippet i personvernforordningen.

Personvernkommisjonen mener at andre myndigheter enn Datatilsynet, bør veilede om alle personvernspørsmål som direkte er knyttet til deres myndighetsområde. Dette er avgjørende for å sikre at disse myndighetene hensyntar personvern i sin virksomhet. *Kommisjonen* understreker at slik veiledning vil komme på toppen av Datatilsynets veiledning. Videre vil Datatilsynet alltid ha tilsynskompetanse.

13.4.7 Betydningen av forvaltningens alminnelige veiledningsplikt

Innenfor sitt saksområde har forvaltningsorganer en alminnelig veiledningsplikt, se forvaltningsloven § 11. Veiledning skal gis for å sette parter og andre interesserte i stand til å vareta sine interesser i bestemte saker. Veiledningsplikten gjelder lover, forskrifter og praksis på vedkommende forvaltningsområde, og regler for saksbehandlingen. Omfanget av veiledningen kan tilpasses forvaltningsorgans situasjon og kapasitet til å påta seg slik virksomhet.

Når det gjelder andre myndigheters veiledningsplikt om personvern, er det i dag uklart om den generelle plikten til å veilede også omfatter personvernregelverket. Paragraf 11 i forvaltningsloven nevner spesielt plikt til å veilede om regler vedrørende saksbehandling i forvaltningsloven. Mange av bestemmelsene i personvernregelverket gjelder saksbehandling knyttet til behandling av personopplysninger, og er i realiteten like viktige rettslige krav til forvaltningens saksbehandling som bestemmelsene i forvaltningsloven.

Personvernkommisjonen mener at, i tillegg til veiledningsansvar om personvernregler for sektorvise tilsynsmyndigheter, bør alle forvaltningsorganer gis tydelig veiledningsansvar i forvaltningsloven § 11 for spørsmål som gjelder behandling av personopplysninger innenfor deres respektive myndighetsområder. Det er viktig at personvernkompetanse og -ressurser finnes i disse tilsynene, slik at de kan ta personvern i betraktning som en integrert del av sine avgjørelser. En utviding av veiledningsansvaret må for øvrig ikke gripe inn i Datatilsynets veiledningsansvar for personvern.

13.4.8 Veiledning i regi av bransjeorganisasjoner, fellesfunksjoner innen offentlig forvaltning med flere

Selv om en gjør maksimalt ut av Datatilsynets veiledningsplikt og utvider og tydeliggjør veiledningsplikten vedrørende personvern for sektorvise tilsynsmyndigheter og offentlige forvaltningsorganer, vil det gjenstå viktige behov for veiledning og tilgang til ekspertise.

Etter *Personvernkommisjonens* syn er det positivt for behandlingsansvarlige og databehandlere å kunne motta veiledning både på bakgrunn av kompetanse om personvern og spesiell sakkunnskap om det saksområdet de driver sin virksomhet. Således vil det for eksempel være hensiktsmessig at IKT-bransjen og mediebransjen søker veiledning og råd fra ekspertise innen egen bransje. Forholdet er tilsvarende innen en rekke andre bransjer, men det vil variere fra bransje til bransje hvor store behovene er. Et lignende behov finnes trolig i offentlig forvaltning.

Samarbeid mellom behandlingsansvarlige om oppbygging av kompetanse og tilbud om veiledningsvirksomhet kan etter *Personvernkommisjonens* syn være en god måte å løse ansvarsprinsippet på. Selv om behandlingsansvarlige får råd om forståelsen av personvernregelverket, er det fremdeles hver behandlingsansvarlig som har ansvaret i henhold til personvernforordningen. Slike samarbeid om veiledningstjenester vil kunne gi bedre etterlevelse av gjeldende regelverk.

En risiko med nevnte former for samarbeid, er at de behandlingsansvarlige kan komme til å opptre med større grad av selvtillit enn om de agerer hver for seg. Dette kan komme til å gi flere tilfeller av uenigheter mellom faglig sterke sammenslutninger på den ene side, og Datatilsynet og andre tilsynsmyndigheter på den annen side. *Person-*

vernkommisjonen mener det ikke er grunn til å unngå slike uenigheter. Tvert imot kan det være en fordel om uenigheter som er prinsipielt viktige, kommer frem og får autoritativ avgjørelse i Personvernnemnda eller i domstolene. Dersom saker der det er uenighet blir avgjort av Personvernnemnda eller domstolene, vil dette lede til rettskraftige avgjørelser og autoritativ avklaring av rettsspørsmålene og større forutberegnelighet.

Hvis slike samarbeidskonstellasjoner har dialog med Datatilsynet, vil det dessuten kunne skjerpe grundigheten og kvaliteten av Datatilsynets analyser. Dersom det ikke er mulig å nå frem til felles standpunkt, og det derfor skulle oppstå restanse av betydning ved Personvernnemda, mener *Personvernkommisjonen* en bør styrke denne nemndas kapasitet for å sikre akseptable saksbehandlingstider.

13.5 Behov for tilsyn fra andre tilsynsmyndigheter

Personvernkommisjonen har ikke gjort noen systematisk gjennomgang av myndighetsområdene for tilsyn som har særlig ansvar innenfor sektorer der behandling av personopplysninger og personvern spiller stor rolle. Arbeidstilsynet og Riksarkivet har imidlertid sin myndighet begrenset til hver sine særlover.[24] Helsetilsynet er eksempel på en tilsynsmyndighet som generelt skal utøve myndighet «i samsvar med det som er bestemt i lover og forskrifter» (se helsetilsynsloven § 4).

Personvernkommisjonen vil peke på at den rollen andre tilsynsmyndigheter har ved håndhevelsen av personvernregelverket varierer fra tilsyn til tilsyn, og synes ikke å være basert på en prinsipiell holdning til spørsmål om myndighetsfordeling og -samarbeid.

Personvernkommisjonen anbefaler at det settes i gang et systematisk arbeid for å styrke sektortilsyns arbeid med personvernregelverket, og for å klargjøre hjemlene for slik utøvelse av myndighet.

Etter *Personvernkommisjonens* syn er det ikke grunn til å se på mulig uenighet mellom sektortilsyn og Datatilsynet som noe problem. Forutsetningen må være at alle tilsyn uansett gjør fullt forsvarlig rettsanvendelse og skjønnsutøvelse. Dessuten vil Datatilsynets praksis og veiledere, Personvernnemdas praksis og uttalelser fra Det europeiske personvernrådet måtte tillegges stor vekt også av sektortilsyn. Videre vil Datatilsynet alltid ha mulighet til å gjennomføre tilsyn. Eventuelle uenigheter på grunn av ulike avveininger av krysssende hensyn, må etter *Personvernkommisjonens* syn ses på som positivt for den helt nødvendige meningsutvekslingen om slike vanskelige spørsmål, og vil i tråd med rettssystemet eventuelt bli avgjort av domstolene.

13.6 Datatilsynets rolle ved utforming av lov og forskrifter

Datatilsynet har mange oppgaver. Tilsynet er ikke bare et myndighetsorgan, men er blant annet også gitt rollen som en slags rådgiver for blant annet regjeringen og Stortinget i spørsmål knyttet til nasjonal lovgivning og administrative tiltak. Slik rådgivning skal gis i samsvar med nasjonal lov. Datatilsynet vil ofte være relevant høringsinstans for lover og forskrifter, jf. henholdsvis utredningsinstruksen punkt 3-3 og forvaltningsloven § 37. I 2020 mottok Datatilsynet 198 høringssaker, og gav uttalelse i 50 av disse sakene.[25]

Personvernforordningen inneholder en regel om at nasjonale myndigheter skal rådføre seg med tilsynsmyndigheten ved utarbeiding av lov og forskrifter, se artikkel 36 nr. 4. I henhold til avsnitt 96 i fortalen til forordningen, er formålet med bestemmelsen blant annet å bidra til å redusere risikoen for registrerte personer. Slike risikoreduserende innspill kan best gis tidlig i lovgivningsprosessen, før fullstendig forslag til bestemmelser er utarbeidet og sendt på høring. I samtale med Datatilsynet har *Personvernkommisjonen* fått innspill om at tilsynet mener at artikkel 36 nr. 4 gir en plikt til å rådføre seg med Datatilsynet ved lovarbeid, ut over den formelle høringsrunden. Ifølge Datatilsynet forstår føderale tyske myndigheter artikkel 36 nr. 4 slik at alle lovarbeider som berører personvern, skal forelegges det tyske tilsynet. Datatilsynet ønsker at prosessen skal reserveres for tilfeller der personvern er et hovedtema og ellers når det er høy risiko etter artikkel 35.

Personvernkommisjonen mener artikkel 36 nr. 4 forutsetter en særskilt rådføringsplikt, slik tidligere kommentert i kapittel 6 og 7. Bestemmelsen kan ikke anses å være etterlevet ved å gi Datatilsynet anledning til å være høringsinstans på linje med den rett enhver virksomhet og borger har etter utredningsinstruksen. Uansett påligger det

[24] I arbeidsmiljøloven § 18-1 heter det for eksempel at «Arbeidstilsynet fører tilsyn med at bestemmelsene i og i medhold av denne lov blir overholdt», og i arkivlova fastsettes det bl.a. at Riksarkivet kan «gje pålegg som er naudsynte for å oppfylla føresegner gjevne i eller i medhald av denne lova, se § 7.

[25] Datatilsynet. (2021). *Årsrapport for 2020.*

regjeringen å utrede lovgivning så omfattende og grundig som nødvendig, og på balansert, systematisk og helhetlig måte når spørsmålene er av prinsipiell karakter.[26]

Personvernkommisjonen mener Datatilsynet må gis adgang til tidlig involvering i lov- og forskriftssaker som reiser prinsipielle spørsmål om personvern og når det er høy risiko for grunnleggende rettigheter og friheter. Etter *kommisjonens* syn, vil det åpenbart gi mest forsvarlig saksutredning dersom Datatilsynets synspunkter blir kjent på et tidlig tidspunkt i lovarbeidet. Hvis argumenter knyttet til ivaretakelse av personvernet kommer tidlig i prosessen, vil det normalt være lettere å ta hensyn til dette enn når synspunktene blir kjent i høringsrunden.

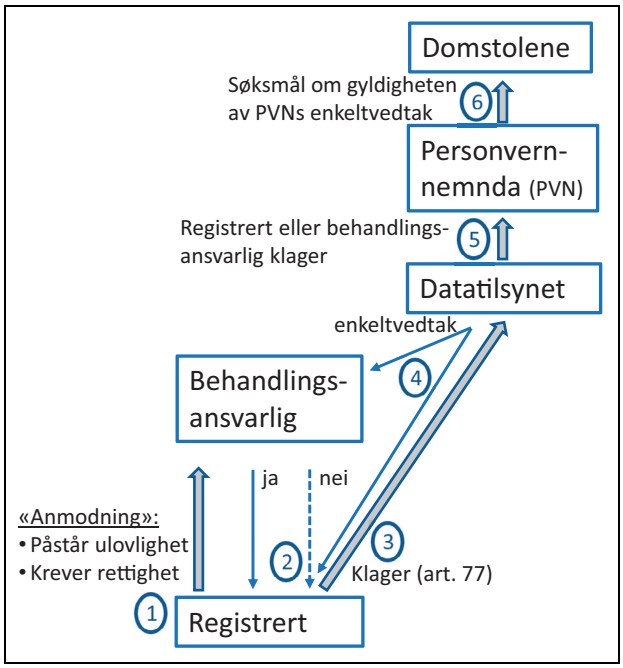
Etter *Personvernkommisjonens* syn vil det normalt være langt mer effektiv bruk av Datatilsynets begrensende ressurser å involvere tilsynet på et tidlig stadium. Personvernforordningen stiller blant annet krav til utforming av nasjonal lovgivning. Tidlig involvering av Datatilsynet i lov- og forskriftsarbeid, kan forenkle saksbehandlingen i vedkommende departement, fordi risikoen for å gjøre feil som må rettes opp blir redusert.

Datatilsynets rolle som rådgiver i lov- og forskriftsprosessen og som høringsinstans, kan ha betydning for hvordan en bedømmer Datatilsynets rolle som tilsyn og myndighet i enkeltsaker. Samtidig som *Personvernkommisjonen* mener det er viktig at Datatilsynet blir tidlig involvert i samsvar med personvernforordningen artikkel 36 nr. 4, og opptrer som høringsinstans i samsvar med utredningsinstruksen og forvaltningsloven, mener *kommisjonen* det er viktig med åpenhet om slike prosesser. Etter *Personvernkommisjonens* syn bør alle Datatilsynets høringsuttalelser gjøres offentlig tilgjengelig på Datatilsynets nettsider. Selv om uttalelsene normalt vil være tilgjengelig på vedkommende departements høringssider, er det vesentlig at det til enhver tid finnes en samlet oppdatert tilgang til slike uttalelser.

13.7 Spesielt om behandling av klager fra registrerte

13.7.1 Oversikt

For enkeltindivider er det av stor betydning å kunne ta opp uenigheter og få avgjort spørsmål som har betydning for personvernet deres. Personvernforordningen inneholder flere ordninger som



Figur 13.1

gir registrerte personer rett til å få spørsmål vurdert og overprøvet. *Personvernkommisjonen* er ikke kjent med at det er gitt samlet oversikt over mulighetene for anmodninger og klager. Spørsmålet er derfor relativt inngående behandlet nedenfor. Ordningene er illustrert i figur 13.1 ovenfor.

Den registrerte kan for det første hevde at en behandling av personopplysninger generelt er ulovlig, for eksempel fordi den mangler behandlingsgrunnlag, fordi formålet for behandlingen er upresist angitt, fordi det ikke er gitt tilstrekkelig informasjon til de registrerte, eller fordi opplysningene ikke er tilstrekkelig sikret. Slike innsigelser vil ha konsekvenser for alle registrerte det blir behandlet opplysninger om. Dersom det generelle behandlingsopplegget er ulovlig overfor én person, vil det sannsynlig også være ulovlig overfor alle personer som er omfattet av behandlingen.

Registrerte personer kan også påstå at opplysninger om dem selv er ukorrekte eller ufullstendige. De kan mene at behandlingsansvarlige ikke har lovlig tilgang til opplysningene om dem, for eksempel fordi det vil stride mot nasjonale bestemmelser om taushetsplikt. Slike påstander har kun direkte betydning for den registrerte som klager. Likevel kan problemstillingen ha indirekte konsekvenser for mange, fordi den konkrete saken kan være uttrykk for svikt i den behandlingsansvarliges systemer og rutiner.

I tilfeller der det generelt eller konkret er påstand om ulovlig behandling, kan registrerte velge å først bringe saken inn for den behand-

[26] Se Finansdepartementet. (2016). *Utredningsinstruksen*, punkt 2-2.

lingsansvarlige i form av en «anmodning», og så eventuelt klage behandlingsansvarliges avgjørelse inn for Datatilsynet (jf. 1, 2 og 3 i figuren). De kan imidlertid også velge å bringe saken direkte inn for Datatilsynet med krav om at Datatilsynet skal avgjøre spørsmålet om lovlighet (jf. 3 i figuren).

En tredje situasjon oppstår når den registrerte retter en anmodning til den behandlingsansvarlige om bruk av sine rettigheter etter artikkel 15–22 (jf. 1 i figuren). Den registrerte ber for eksempel om innsyn, eller om at visse opplysninger blir slettet eller ikke blir behandlet. Behandlingsansvarlige skal normalt gi svar innen én måned fra anmodningen om bruk av rettigheter ble mottatt (jf. 2 i figuren). Dersom den registrertes ønske ikke etterkommes, skal den behandlingsansvarlige redegjøre for årsaken til nektelsen og opplyse om adgangen til å klage til Datatilsynet.

Datatilsynet plikter å ta stilling til klager fra den registrerte i alle tre nevnte sakstyper. Avgjørelsen blir et enkeltvedtak i forvaltningslovens forstand (jf. 4 i figuren). Før vedtak plikter Datatilsynet å sørge for at saken er utredet på forsvarlig måte.

Hvis behandlingsansvarlige eller den registrerte er misfornøyd med Datatilsynets enkeltvedtak, kan vedtaket klages inn for Personvernnemnda i samsvar med reglene om klage i personopplysningsloven og forvaltningsloven (jf. 5 i figuren). Spørsmål om gyldigheten av Personvernnemndas enkeltvedtak kan eventuelt bringes inn for domstolene (jf. 6 i figuren).

13.7.2 Synligheten av registrertes rett til å klage til Datatilsynet

Personvernforordningen artikkel 77 gir generell rett for registrerte personer til å klage til tilsynsmyndigheten og lyder:

> «enhver registrert [skal] ha rett til å klage til en tilsynsmyndighet […] dersom den registrerte anser at behandlingen av personopplysninger som gjelder vedkommende, er i strid med denne forordning.»

Denne bestemmelsen gir de registrerte en rett til direkte klage til Datatilsynet dersom de anser en behandling for å være ulovlig, uten først å ta saken opp med den behandlingsansvarlige. Den gir også rett til å klage avgjørelser behandlingsansvarlige har tatt om bruk av rettigheter, og eventuelt andre spørsmål, inn for Datatilsynet. Det fremgår av personvernforordningen artikkel 80 nr. 1 at den registrerte kan gi en ideell organisasjon fullmakt til å klage på sine vegne, herunder klage etter artikkel 77.

Personvernombud har ingen formell rolle i klagesaker. Riktignok kan registrerte personer kontakte personvernombudene for å få informasjon om behandling av personopplysninger i virksomheten og utøvelse av rettigheter. Personvernombudene skal imidlertid, verken formelt eller reelt, treffe avgjørelser ved uenighet mellom registrerte og den virksomhet de er personvernombud for. Imidlertid kan ombudene stille generelle spørsmål ved om den behandlingsansvarlige etterlever regler om klage på tilstrekkelig måte.

Kapittel 6 i personopplysningsloven har egne norske regler om klage. Bestemmelsen om klage på Datatilsynets enkeltvedtak fremgår av personopplysningsloven § 22 annet ledd. Dette er en klagebestemmelse som primært gir rettssikkerhet for behandlingsansvarlige, men gir også rettigheter for registrerte personer.

Reglene om den registrertes klagerett på avgjørelser som er truffet av behandlingsansvarlige vedrørende om en behandling er ulovlig, eller om bruk av rettigheter, er verken gjengitt eller vist til i personopplysningsloven. Dette til tross for at de er meget viktige for de registrertes personvern og rettssikkerhet. Bare spesialister vil reelt sett være i stand til å finne frem til reglene om registrertes rett til å klage i personvernforordningen artikkel 77.

Personvernkommisjonen mener det er uheldig at personopplysningsloven ikke på tydelig måte slår fast den retten registrerte personer har til å få spørsmål vurdert og overprøvet. Slik klargjøring er viktig for å styrke registrerte personers rettsstilling. Personvernforordningen er neppe til hinder for at reglene om registrertes rettigheter delvis blir gjentatt og vist til i kapitlet om klage i personopplysningsloven. *Kommisjonen* viser her til uttalelsen i avsnitt 8 i fortalen til forordningen, som åpner for at det kan innføres presiseringer eller begrensninger av regler i nasjonal rett for å gjøre nasjonale bestemmelser forståelige for de personer de får anvendelse på.

Personvernkommisjonen merker seg at Datatilsynet ikke har utformet rutine for å inngi klage fra registrerte personer.

Personvernkommisjonen slår fast at det er en stor utfordring for Datatilsynet at de mottar store mengder klager fra registrerte personer. Slike arbeidsoppgaver kan ses som mindre effektiv bruk av personalressurser enn saker som gjelder systemløsninger med virkning for et stort antall mennesker. Det er likevel uheldig for rettsbeskyt-

telsen dersom det ikke er lagt godt til rette for klage når det er uenighet mellom en registrert og en behandlingsansvarlig. På lignende måte som behandlingsansvarlige plikter å legge til rette for at registrerte kan utøve sine rettigheter, bør også Datatilsynet legge bedre til rette for bruk av retten til å klage til dem. *Personvernkommisjonen* ser derfor positivt på at Datatilsynet er i ferd med å utvikle et digitalt klageskjema.

Etter *Personvernkommisjonens* mening er det ikke tilfredsstillende med saksbehandlingstider på fra tre til seks måneder, eller mer, for behandling av klager fra enkeltpersoner som mener deres personvern er krenket. Slik lang saksbehandlingstid kan for eksempel føre til at en ulovlig behandling av personopplysninger får fortsette i lang tid, med mulige spredningseffekter, fordi opplysningene deles i en kjede av aktører. *Kommisjonen* mener en slik situasjon ikke gir forsvarlig saksbehandling, og gir plikt for Datatilsynet til å treffe effektive tiltak for å bedre situasjonen. Trolig vil et digitalt klageskjema gjøre det mulig å avgjøre enkle saker betydelig raskere enn i dag, innen den lovfastsatte fristen.

13.7.2.1 Registrertes klagerett og ansvarsprinsippet

Prinsippet om den behandlingsansvarliges ansvar er grunnleggende i personvernforordningen. Prinsippet innebærer at det er den behandlingsansvarlige som skal sørge for at personvernprinsippene blir overholdt, og at det blir truffet nødvendige tiltak for at bestemmelsene i personvernforordningen om blant annet behandlingsansvarliges plikter blir etterlevet.

Det er et grunnleggende personvernprinsipp at den behandlingsansvarlige skal treffe tiltak for å sikre rettferdighet og åpenhet. Dette betyr blant annet at behandlingsansvarlige må sikre at anmodninger de får fra registrerte personer, med påstand om ulovligheter og ønske om bruk av rettigheter, blir vurdert på saklig og balansert måte.

Behandlingsansvarlige skal legge til rette for bruk av rettighetene i personvernforordningen artikkel 15–22, og skal informere om rettighetene på en klar og forståelig måte. I tillegg gjelder det generelle bestemmelser om at behandlingsansvarlige blant annet skal bygge personvernprinsipper og rettigheter inn i tekniske løsninger, jf. «innebygd personvern» i artikkel 25 nr. 1. Dette gjelder også innbygging for å understøtte retten registrerte har til å be den behandlingsansvarlige om endring av ulovlige forhold, bruk av rettigheter, og retten til å klage behandlingsansvarliges avgjørelse inn til Datatilsynet. Løsningene må være tilgjengelige digitalt.

Krav til innebygd personvern er betinget av at tiltaket står i et rimelig forhold til kostnader, arten og omfanget av opplysningene som blir behandlet, og risikoen for krenkelse av personers rettigheter og friheter. Man skal dessuten ta hensyn til den tekniske utviklingen, og det er neppe grunnlag for å kreve annet enn standard teknologi.

Personvernkommisjonen har ikke gjennomført systematiske undersøkelser av innebygd personvern som nevnt ovenfor. Likevel er det klare, generelle inntrykket at slike tiltak forekommer meget sjelden. En slik tilstand er ikke i tråd med personvernforordningen.

13.7.2.2 Betydningen av Datatilsynets ansvar

Samtidig som det gjelder et strengt ansvarsprinsipp for behandlingsansvarlige, har Datatilsynet ansvar for å føre tilsyn med at bestemmelsene i forordningen, herunder reglene om registrertes rettigheter, blir etterlevet. Det er altså et viktig samspill mellom ansvarsprinsippet og Datatilsynets tilsyn og mulighet for å gi pålegg om å treffe tiltak for etterlevelse av forordningen.

Selv om ansvarsprinsippet tilsier at alle behandlingsansvarlige skal ha rutiner som understøtter registrertes rett til å sende anmodninger til behandlingsansvarlige, gir dette neppe tilstrekkelig virkning alene. I tillegg er det viktig at Datatilsynet arbeider aktivt for å bidra til at praksis er i samsvar med gjeldende regler.

Det er svært arbeidskrevende å føre tilsyn med at alle behandlingsansvarlige etterlever de aktuelle bestemmelsene. En alternativ tilnærming kan være at Datatilsynet bruker generelle virkemidler. For eksempel er det mulig å oppfordre bransjeorganisasjoner og andre til å utarbeide atferdsnormer der det blir stilt spesifikke krav til eksistensen av og innholdet i internettbaserte rutiner som skal understøtte registrertes rett til å sende anmodning til behandlingsansvarlige. Datatilsynet har myndighet til å godkjenne slike atferdsnormer, men det vil i stor grad være opp til bransjene selv å håndheve kravene. Også sertifiseringsordningen i forordningen kan gi lignende effekter.

Behandlingsansvarlige kan imøtekomme eller avslå registrertes anmodning om å rette ulovlige forhold og om bruk av rettigheter. Dette gir situasjoner med «bukken og havresekken», fordi den behandlingsansvarlige treffer avgjørelser om uenigheter de selv er part i. Selv om den behandlingsansvarlige har gode intensjoner, sier det seg

selv at det vil være meget vanskelig å opptre helt nøytralt.

Det skjeve maktforholdet innebærer ikke at alle avgjørelser som går i den registrertes disfavør, er uriktige eller urimelige. Imidlertid kan det skjeve forholdet gi grunnlag for stor skepsis fra registrerte personer til behandlingsansvarliges avgjørelse. Dermed kan det oppstå et større behov for å bringe saken inn for avgjørelse i Datatilsynet enn dersom tilliten hadde vært større. Større tillit til avgjørelser truffet av behandlingsansvarlige vil med andre ord kunne dempe behovet for å klage til Datatilsynet.

I internettbaserte rutiner, som nevnt ovenfor, må det derfor være mekanismer som bidrar til at saker som behandlingsansvarlige avgjør (om for eksempel påstått ulovlig behandling, innsyn, sletting eller behandlingsgrunnlag) blir tatt stilling til på mest mulig balansert måte. Et eksempel på tiltak som kan virke i retning av balanserte avgjørelser, er dersom den behandlingsansvarlige har en fast person som behandler anmodninger fra registrerte. Dette vil både kunne innebære tilstrekkelig kompetanse og profesjonalisering, og sikre at personen(e) har god oversikt over praksis. Det kan også tydeliggjøres at det primært er den behandlingsansvarlige som skal utrede saker som registrerte personer reiser, og dermed har ansvar for at saken er opplyst fra begge sider. Eventuelt kan det gis en eksplisitt plikt til å la den registrerte komme til orde på bestemte måter, for eksempel med bistand fra fullmektig eller en ideell organisasjon.

Et ytterligere element i rutiner for tilfredsstillende behandling av anmodninger fra registrerte personer, kan være å stille krav til dokumentasjon av behandlingsansvarliges praksis i slike saker. Dokumentasjonen kan blant annet vise i hvilken grad saker blir klaget inn til Datatilsynet og omgjort. Innrapporterte tall kan i sin tur gi grunnlag for Datatilsynets prioriteringer av hvor de skal utføre tilsyn. Mekanismer som gjør at de behandlingsansvarliges avgjørelser blir monitorert, med mulige konsekvenser for tilsyn og kontroll, kan tenkes å være sterkt motiverende for den behandlingsansvarliges noenlunde balanserte behandling av krav fra den registrerte.

Etter personvernforordningen kan hvert land fastsette myndighet i nasjonal lov ut over det som gjelder etter personvernforordningen, se artikkel 58 nr. 6. Det vil derfor trolig være adgang til å fastsette enkelte norske bestemmelser om Datatilsynets myndighetsutøvelse i saker der det er uenighet mellom registrerte personer og behandlingsansvarlige.

Personvernkommisjonen antar at atferdsnormer, standarder og IT-verktøy med innebygde løsninger, kombinert med nasjonale lov- og forskriftsbestemmelser, kan gjøre registrertes rett til å anmode den behandlingsansvarlige om å vurdere lovlighet og bruke rettigheter, vesentlig mer effektiv enn i dag. *Kommisjonen* antar at summen av slike virkemidler kan gjøre at færre uenigheter mellom registrerte og behandlingsansvarlige ender opp som klagesaker hos Datatilsynet.

13.8 Personvernkommisjonens anbefalinger oppsummert

- *Personvernkommisjonen* anbefaler at regjeringen arbeider for å opprette tilsynsmyndigheter på europeisk nivå med myndighet og ansvar for å sørge for effektiv håndhevelse av personvernregelverket overfor de globale plattformaktørene, tilsvarende bestemmelsene som er inntatt i Digital Markets Act.
- *Personvernkommisjonen* mener det bør gjøres jevnlige evalueringer av Personvernnemda. Evalueringene bør se på om nemda utfører sin funksjon på tilstrekkelig vis, og at den er velfungerende.
- *Personvernkommisjonen* mener det er et klart behov for å styrke Datatilsynet. Personvernet kan imidlertid ikke kun sikres ved en sterk, sentral tilsynsmyndighet. *Personvernkommisjonen* mener derfor det må skje en samtidig styrking av andre viktige samfunnsaktørers forutsetninger for å bidra til et godt personvern.
- *Personvernkommisjonen* mener det er svært positivt at norske tilsyn samarbeider for å beskytte forbrukernes rettigheter. Dette samarbeidet bør sikres for fremtiden.
- *Personvernkommisjonen* mener andre tilsynsmyndigheter med ansvarsområder som har stor og direkte betydning for ivaretakelse av personvern kan spille en større rolle for personvernet enn de gjør i dag. For eksempel må Arbeidstilsynet både kunne føre tilsyn med arbeidsgivers kontrolltiltak etter bestemmelsene i arbeidsmiljøloven, og samtidig anvende de generelle reglene i personvernforordningen som aktualiseres av kontrolltiltaket.
- *Personvernkommisjonen* mener det er viktig at det etableres tydelige rammer for henholdsvis veiledning og tilsyn i Datatilsynet. *Kommisjonen* mener det kan være hensiktsmessig at tilsynet organiserer seg slik at en behandlingsansvarlig ikke risikerer å få tilsyn basert på infor-

masjon som stammer fra dialog knyttet til Datatilsynets veiledning av virksomheten.

- *Personvernkommisjonen* mener at dersom Datatilsynets sandkasse skal videreføres, bør spørsmålene som en tar stilling til i hvert prosjekt legges åpent frem for mulige merknader før konklusjonene treffes. I konklusjonene bør en i tillegg legge stor vekt på å få frem forutsetninger og eventuell tvil knyttet til konklusjonene. Generelt bør rapportene legges opp slik at de i minst mulig grad blir oppfattet som forhåndsavgjørelser.
- *Personvernkommisjonen* mener andre myndigheter enn Datatilsynet bør veilede om personvernspørsmål som direkte er knyttet til deres myndighetsområde. Dette er avgjørende for å sikre at disse myndighetene hensyntar personvern i sin virksomhet. *Kommisjonen* understreker at slik veiledning vil komme på toppen av Datatilsynets veiledning. Videre vil Datatilsynet alltid ha tilsynskompetanse.
- *Personvernkommisjonen* mener alle forvaltningsorganer bør gis tydelig veiledningsansvar i forvaltningsloven § 11 for spørsmål som gjelder behandling av personopplysninger innenfor deres respektive myndighetsområder. En utviding av veiledningsansvaret må ikke gripe inn i Datatilsynets lovbestemte veiledningsansvar.
- *Personvernkommisjonen* anbefaler at det settes i gang et systematisk arbeid for å styrke sektortilsynenes arbeid med personvernregelverket, og for å klargjøre hjemlene for slik utøvelse av myndighet.
- *Personvernkommisjonen* mener artikkel 36 nr. 4 forutsetter en særskilt rådføringsplikt. Bestemmelsen kan ikke anses å være etterlevet ved å gi Datatilsynet anledning til å være høringsinstans på linje med den rett enhver virksomhet og borger har etter utredningsinstruksen. Uansett påligger det regjeringen å utrede lovgivning så omfattende og grundig som nødvendig, og på en balansert, systematisk og helhetlig måte når spørsmålene er av prinsipiell karakter.
- *Personvernkommisjonen* mener Datatilsynet må gis adgang til tidlig involvering i lov- og forskriftssaker som reiser prinsipielle spørsmål om personvern og når det er høy risiko for grunnleggende rettigheter og friheter. Etter *Personvernkommisjonen*s syn, vil det åpenbart gi mest forsvarlig saksutredning dersom Datatilsynets synspunkter blir kjent på et tidlig tidspunkt i lovarbeidet. Hvis argumenter knyttet til ivaretakelse av personvernet kommer tidlig i prosessen, vil det normalt være lettere å ta hensyn til dette enn når synspunktene blir kjent i høringsrunden.
- *Personvernkommisjonen* anbefaler at alle Datatilsynets høringsuttalelser bli gjort offentlig tilgjengelig på Datatilsynets nettsider. Selv om uttalelsene normalt vil være tilgjengelig på vedkommende departements høringssider, er det et vesentlig at det til enhver tid finnes en samlet oppdatert tilgang til slike uttalelser.
- *Personvernkommisjonen* mener det er uheldig at personopplysningsloven ikke tydelig slår fast den retten registrerte personer har til å få spørsmål vurdert og overprøvet. Slik klargjøring er viktig for å styrke registrerte personers rettsstilling.

Kapittel 14
Økonomiske og administrative konsekvenser

14.1 Innledning

Det følger av mandatet at økonomiske, administrative og andre vesentlige konsekvenser av utvalgets forslag skal utredes og fremgå av utredningen i samsvar med utredningsinstruksen.

Svært mange av *Personvernkommisjonens* anbefalinger dreier seg om å etablere rutiner og prosesser for å etterleve personvernregelverket på en mer effektiv måte enn i dag. Flere forslag dreier seg om å tydeliggjøre og forsterke det behandlingsansvaret ledelsen i virksomhetene allerede har. Spesielt gjennom å prioritere og følge opp rutiner og prosesser for å ivareta de registrertes personvern. Disse anbefalingene innebærer ikke ny virksomhet – de handler om å følge eksisterende regelverk. Etterlevelse vil fordre en tydeligere prioritering internt. Hvilke prioriteringer som må gjøres, og hvilke økonomiske og administrative konsekvenser dette eventuelt vil kunne få, har ikke *kommisjonen* hatt grunnlag for å vurdere.

Noen av *kommisjonens* tiltak dreier seg om ny virksomhet, og disse tiltakene vil ha økonomiske og administrative konsekvenser. De fleste av disse forslagene må imidlertid utredes nærmere. De økonomiske og administrative konsekvensene av forslagene vil avhenge av utforming og omfang av de tiltakene som blir besluttet gjennomført. Noen av tiltakene innebærer endringer i administrative prosesser uten vesentlig økonomisk merkostnad, andre tiltak forutsettes å kunne iverksettes ved omprioriteringer innenfor gjeldende budsjetter, mens noen større tiltak vil kreve betydelig økte budsjettrammer. Da det ikke har vært mulig innenfor *kommisjonens* funksjonstid å utrede alle tiltakene, må derfor departementet foreta nødvendige konsekvensvurderinger i forbindelse med en eventuell oppfølging av de ulike tiltakene.

Tiltakene *Personvernkommisjonen* foreslår vil i hovedsak kreve midler til drift, prosjektgjennomføring eller utredning. Andre tiltak vil kreve at det bevilges midler til kompetanseheving, eller at det gjennomføres administrative grep. Selv om flere av tiltakene vil kreve tilføring av ekstra midler, vil også flere av tiltakene ha en samfunnsmessig og økonomisk gevinst. For eksempel vil mer grundige vurderinger av personvernkonsekvenser og styrking av kompetanse og ressurser ha en kostnadsside, men tiltak for å bedre personvernet vil også ha en samfunnsøkonomisk gevinst, blant annet i form av effektivisering og tillit til løsningene som utvikles, i et lengre perspektiv. Anbefalinger om å profesjonalisere og sentralisere personvernkompetanse vil medføre kostander med å bygge opp eller styrke eksisterende strukturer, men på lengre sikt vil bedre koordinering av personvernarbeidet medføre samfunnsøkonomiske gevinster, blant annet i form av at mer effektive prosesser.

14.2 Den digitale forvaltningen

- Opprettelse av et rådgivende og frittstående organ for forvaltningen som skal vurdere og drøfte prinsipielle og generelle spørsmål knyttet til bruk av personopplysninger i offentlig forvaltning, vil innebære utgifter til etablering og drift. Det vil også medføre administrative konsekvenser i form av etablering av rutiner og retningslinjer for organet.
- Anbefalingen om at tiltaket «Felles sikkerhet i forvaltningen» gis prioritet som et sentralt finansiert tiltak, og at virksomheter med tilgrensende ansvarsområder gis oppdrag i tildelingsbrev om å bidra inn i dette arbeidet, vil medføre omprioriteringer hos disse virksomhetene og potensielt en økning i utgiftene.
- Videreutvikling av standarder for deling av personopplysninger vil medføre kostnader. I et lengre perspektiv vil imidlertid eksistensen av standarder bidra til mer effektiv ressursbruk. Det samme gjelder *kommisjonens* forslag om at virksomhetene i forvaltningen må få tydeligere anbefalinger (eller «norm») for styringsaktiviteter. Det vil medføre utgifter å få en norm på plass, men en norm vil bidra til å effektivisere

prosesser og tilhørende ressursbruk, samt redusere personvernrisiko ved å øke kvaliteten på prosessene.
- Utredning av om en samtykkebasert gjennomføring av «kun-én-gang»-prinsippet vil avhjelpe personvernulemper som oppstår ved deling av personopplysningen mellom offentlige etater. Dette vil kreve prosjektmidler.
- Oppdatering av veilederen om lovteknikk og -lovforberedelse («lovteknikkheftet») vil kreve prosjektmidler.
- Styrking av personvernkompetansen til ledere, saksbehandlere og andre ansatte som har behov for slik kompetanse i offentlig forvaltning, vil kreve at forvaltningen omprioriterer ressurser eller får tilført økte ressurser.
- Forslag om at departementene i større grad rådfører seg med Datatilsynet ved lovarbeider vil kreve tilføring av mer ressurser til Datatilsynet for å kunne prioritere arbeidet. Samtidig vil forslaget bidra til at lovarbeider utredes bedre på et tidlig stadium, som vil effektivisere de videre prosessene.

14.3 Justissektoren

- Forskning på samfunnsmessige konsekvenser av overvåkningstiltak i justissektoren vil kreve tilføring av forskningsmidler gjennom statsbudsjettet.
- Anbefalingen om å nedsette et utvalg for å utrede metodebruken i justissektoren vil innebære kostnader ved å oppnevne og honorere utvalget samt kostnader til sekretariat.
- Styrking og endring av Kommunikasjonskontrollutvalgets mandat vil innebære tilføring av ekstra budsjettmidler i form av opprettelse av ekstra stillinger og kompetansebygging, og administrative konsekvenser i form av endrede rutiner som følge av endring i mandatet. Det vil også innebære kostnader å utrede hvilken konkret kompetanse utvalget behøver, samt hvordan arbeidet med et utvidet mandat bør gjennomføres.
- Styrking av personvernkompetansen i politiet vil kreve ressurser til kompetansebygging og økning eller omprioritering av politiets opplæringsressurser.
- Styrking av undervisningen i personvern ved Politihøgskolen vil medføre at Politihøgskolen må utarbeide nye undervisningsplaner og få tilført ekstra budsjettmidler, eventuelt omdisponere eksisterende midler.
- En utredning av en mulig ny ordning for filtrering av overskuddsinformasjon ved beslag av digitale lagringsmidler, vil kreve utredningsmidler. Dersom en ordning skal etableres, vil det kreve ressurser til etablering og opprettholdelse av ordningen.
- Etablering av en samhandlingsplattform for dokumentutlevering i justissektoren, vil kreve tilføring av budsjettmidler. Plattformen vil imidlertid kunne skape gevinster og besparelser på sikt ved å bidra til mer effektiv samhandling.
- Etableringen av en norm for IKT-sikkerhet vil medføre etableringskostnader, men vil være besparende på sikt ved å forebygge sikkerhetsbrudd.
- Prioritering av IKT-sikkerhet og innebygd personvern ved bestilling og utvikling av løsninger vil øke kostnaden ved enkelte anskaffelser, men vil på sikt føre til besparelser i form av reduksjon av sårbarheter som kan medføre kostbare sikkerhets- og personvernbrudd.
- Anbefalingen om at det bør vurderes om dagens domstolskontroll av politiets tiltak bør utvides til å omfatte flere tiltak enn i dag, vil innebære utredningskostnader.
- Forslag om vurderinger av å implementere bestemmelser fra politidirektivet i politiregisterloven, samt forslaget om å innføre et tillegg i straffeprosessloven § 170a, vil medføre utredningskostnader.

14.4 Skole- og barnehagesektoren

- Utarbeidelse av en personvernnorm for skole- og barnehagesektoren vil medføre kostnader for normarbeid. Det vil imidlertid være kostnadsbesparende over tid ved å bidra til mer effektive og samkjørte rutiner, samt redusere risikoen for kostbare personvernbrudd.
- Etableringen eller videreutviklingen av et nasjonalt test- og kompetansemiljø vil innebære kostnader knyttet til etablering og drift av miljøet, eller bemannings- og kompetansebyggingskostnader dersom det legges til eksisterende strukturer.
- Opplæring av lærere og barnehagelærere i personvern vil medføre utgifter til opplæring, men vil medføre lavere risiko for kostbare personvernbrudd.
- En utredning av digitale verktøy som er i bruk i norsk skole i dag, og hvordan det påvirker personvernet, vil medføre utredningskostnader. En personvernvennlig anskaffelsespolitikk vil medføre økonomiske konsekvenser

ved at skole- og barnehagesektoren i mindre grad vil kunne ta i bruk digitale «gratisløsninger» eller rimeligere alternativer hvor personopplysninger samles inn.
- Eventuelle statlige investeringer i utviklingen av personvernvennlige løsninger for skole- og barnehagesektoren vil medføre investeringskostnader.
- Innføringen av krav til personvern og informasjonssikkerhet i den planlagte nasjonale tjenestekatalogen for digitale læringsmidler vil medføre kostnader for kompetansebygging i Utdanningsdirektoratet, samt kostnader knyttet til testing av løsninger både ved etablering og på løpende basis.
- Opplæring i personvern som grunnleggende menneskerettighet vil medføre administrative konsekvenser ved endring i læreplaner.

14.5 Forbrukerområdet

- Å legge ansvaret for håndheving av informasjonskapsler og lignende sporingsteknologi til Datatilsynet vil kreve økte midler til tilsynet.
- Informasjon og kontrollrutiner hos importører, forhandlere og bransjeorganisasjoner for å sikre personvernet i tilkoblede forbrukerprodukter, vil medføre økonomiske og administrative konsekvenser for bransjeaktørene. Bransjestandarder og merkeordninger vil ha en etableringskostnad, men kan medføre lavere kostnader for enkeltaktører.
- En utredning av konsekvensene ved et forbud mot atferdsbasert markedsføring vil medføre utredningskostnader. Et eventuelt forbud mot atferdsbasert markedsføring mot barn vil ha økonomiske konsekvenser for aktører som selger annonser og som ellers benytter seg av slik teknologi.
- Strenge informasjons- og åpenhetskrav rettet mot plattformer vil medføre kostnader for plattformene det gjelder, for å utvikle, implementere og drifte løsningene.
- Krav om at virksomheter som bruker maskinlæringssystemer for å profilere og segmentere forbrukere, må rapportere om tiltak for å motvirke diskriminering, vil medføre økonomiske og administrative konsekvenser for virksomhetene det gjelder.
- Nye krav for Oljefondets investeringer for å ivareta personvernet, vil medføre økonomiske konsekvenser for Oljefondet. Utarbeidelse av nye forventningsdokumenter vil ha administrative konsekvenser.
- Arbeid for å utrede hvordan konkurranseloven kan anvendes for å forhindre negative personvernkonsekvenser ved oppkjøp og fusjoner, vil medføre utredningskostnader.
- Nedsettelsen av et lovutvalg for å gjennomgå og forslå endringer i regelverk for å beskytte barn og unge i digitale flater vil medføre økonomiske og administrative konsekvenser i nedsettelsen, gjennomføringen og oppfølgingen av lovutvalget.
- Kompetansehevende tiltak knyttet til deling av innhold på nett rettet mot barn og foreldre vil medføre kostnader ved at ressurser må bevilges til for eksempel Datatilsynet og Utdanningsdirektoratet.
- Utvikling av en veileder for barn og foreldre for å styrke forståelsen av barns rett til personvern i familiære forhold, vil medføre prosjektkostnader for Barneombudet.

14.6 Andre områder

- Innføring av nye bestemmelser i ny forvaltningslov som inneholder klare plikter for innebygd personvern, vil medføre kostnader knyttet til lovarbeid.
- Etablering av plikter for undervisningsinstitusjoner til å ha innsyns- og informasjonsrutiner for elever og studenter, for eksempel gjennom opplæringslova og universitets- og høgskoleloven, vil ha økonomiske kostnader ved innarbeiding av rutiner og systemer, samt administrative kostnader for institusjonene og knyttet til lovarbeid.
- Stimulering til utvikling av norsk personvernteknologi vil medføre kostnader for myndighetene. Anskaffelseskrav i offentlig sektor vil føre til økte kostnader i anskaffelser, men vil kunne være kostnadsbesparende på sikt ved å redusere risikoen for kostbare personvernbrudd. Økte forskningsmidler for å fremme personvernfremmende teknologi og midler gjennom forskjellige bevilgningsordninger, vil også ha økonomiske kostnader.
- Innføring av et spesielt vern for personer som utsettes for helt automatiserte avgjørelser i tråd med forordningens regler, inkludert dokumentasjon av systemer og ordninger med manuell vurdering og overprøving, vil medføre administrative konsekvenser i form av etablering av nye rutiner, samt økonomiske konsekvenser knyttet til kompetanseheving og utarbeiding av plikter.

- Innføring av tiltakene fra Digitaliseringsdirektoratets utredning om tilgjengeliggjøring av informasjon om behandling av personopplysninger vil medføre økonomiske kostnader knyttet til etablering og vedlikehold av systemet, samt administrative konsekvenser ved å implementere og iverksette systemet.
- En generell styrking av Datatilsynet vil medføre økonomiske kostnader.
- Utvidet ansvar for personvern hos forskjellige sektortilsyn vil ha administrative konsekvenser ved å omorganisere tilsynenes arbeid, samt økonomiske kostnader ved å bygge kompetanse på personvern i sektortilsynene.
- Klargjøring av hjemler for at sektortilsyn kan utøve myndighet på personvern, vil ha administrative konsekvenser ved utforming av hjemler.
- Endringer ved Datatilsynets sandkasse for kunstig intelligens, vil medføre administrative konsekvenser ved utarbeidelse av nye rutiner i Datatilsynet.
- Kompetansebygging på EU- og EØS-rett i forvaltningen vil ha økonomiske konsekvenser i forbindelse med opplæring av ansatte, men vil kunne føre til besparelser på sikt, ved at lovarbeidsprosesser blir mer solide og effektive.
- En vurdering av om det skal gis nasjonale regler som opprettholder, eventuelt innfører nye vilkår for behandling av genetiske, biometriske og helseopplysninger, vil medføre økonomiske og administrative konsekvenser knyttet til utredningsarbeid.
- Tiltaket om at regjeringen bør legge til rette for etablering av ideelle organisasjoner med allmenne formål å arbeide for personvern, vil ha økonomiske og administrative konsekvenser ved at det må utredes hvordan nasjonalt regelverk kan legge til rette for at ideelle organisasjoner blant annet kan opptre på vegne av registrerte personer, og hvilke krav som bør stilles til organisering og drift av slike foreninger.

Referanser og litteratur

Offentlige utredninger:

NOU 1974: 22 *Persondata og personvern*.
NOU 1975: 10 *Offentlige persondatasystem og personvern*.
NOU 2000: 29 *GMO-mat – Helsemessige konsekvenser ved bruk av genmodifiserte næringsmidler og næringsmiddelingredienser*.
NOU 2003: 21 *Kriminalitetsbekjempelse og personvern – Politiets og påtalemyndighetens behandling av opplysninger*.
NOU 2009: 1 *Individ og integritet – Personvern i det digitale samfunnet.*
NOU 2009: 15 *Skjult informasjon – åpen kontroll. Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker.*
NOU 2011: 20 *Ungdom, makt og medvirkning.*
NOU 2019: 5 *Ny forvaltningslov – Lov om saksbehandlingen i offentlig forvaltning (forvaltningsloven)*.
NOU 2019: 9 *Fra kalveskinn til datasjø – Ny lov om samfunnsdokumentasjon og arkiver*.
NOU 2020: 11 *Den tredje statsmakt – Domstolene i endring*.
NOU 2020: 14 *Ny barnelov – Til barnets beste.*
NOU 2021: 3 *Barneliv foran, bak og i skjermen – Utvalg for beskyttelse av barn og unge mot skadelig medieinnhold – med særlig vekt på pornografisk og seksualisert innhold.*

Lovproposisjoner:

Ot.prp. nr. 108 (2008–2009) *Om lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)*
Prop. 151 L (2009–2010) *Endringar i forvaltningslova og straffegjennomføringslova*.
Prop. 47 L (2011–2012) *Endringer i personopplysningsloven*.
Prop. 68 L (2015–2016) *Endringer i straffeprosessloven mv. (skjulte tvangsmidler)*.
Prop. 56 LS (2017–2018) *Lov om behandling av personopplysninger (personopplysningsloven)*.
Prop. 145 L (2020–2021) *Endringar i opplæringslova, friskulelova og barnehagelova (behandling av personopplysningar, fjernundervisning o.a.)*
Prop. 166 L (2020–2021) *Endringer i forvaltningsloven m.m. (utvidet adgang til informasjonsdeling)*.
Prop. 1 S (2021–2022) *For budsjettåret 2022 under Kommunal- og distriktsdepartementet.*

Innstillinger:

Innst. 243 S (2011–2012) *Innstilling fra kontroll- og konstitusjonskomiteen om sak om hjemmelsgrunnlaget for INFOFLYT-registeret.*
Innst. 186 S (2013–2014) *Innstilling til Stortinget fra kontroll- og konstitusjonskomiteen om Grunnlovsforslag om grunnlovfesting av sivile og politiske menneskerettigheter (unntatt romertallene X og XXIV)*.

Stortingsmeldinger:

Meld. St. 42 (2004–2005) *Politiets rolle og oppgaver*. Justis- og beredskapsdepartementet.
Meld. St. 27 (2015–2016) *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet*. Kommunal- og distriktsdepartementet.
Meld. St. 25 (2018–2019) *Framtidas forbrukar – grøn, smart og digital.* Barne- og familiedepartementet.
Meld. St. 29 (2019 –2020) *Politimeldingen – et politi for fremtiden*. Justis- og beredskapsdepartementet.
Meld. St. 22 (2020–2021) *Data som ressurs – Datadrevet økonomi og innovasjon*. Kommunal- og distriktsdepartementet.

Lover:

Lov 17. mai 1814 Kongeriket Norges Grunnlov, (Grunnloven)
Personregisterloven (opphevet). (1978). *Lov om personregistre m.m.* (LOV-1978-06-09-48).
Arkivlova. (1992). *Lov om arkiv* (LOV-1992-12-04-126).

Opplæringslova. (1998). *Lov om grunnskolen og den vidaregåande opplæringa* (LOV-1998-07-17-61).

Menneskerettsloven. (1999). *Lov om styrking av menneskerettighetenes stilling i norsk rett* (LOV-1999-05-21-30).

Personopplysningsloven (opphevet). (2000). *Lov om behandling av personopplysninger* (LOV-2000-04-14-31).

Straffegjennomføringsloven. (2001). *Lov om gjennomføring av straff mv.* (LOV-2001-05-18-21).

Forbrukerkjøpsloven. (2002). *Lov om forbrukerkjøp* (LOV-2002-06-21-34).

Ekomloven. (2003). *Lov om elektronisk kommunikasjon* (LOV-2003-07-04-83).

Privatskolelova. (2003). *Lov om private skolar med rett til statstilskot* (LOV-2003-07-04-84).

Konkurranseloven. (2004). *Lov om konkurranse mellom foretak og kontroll med foretakssammenslutninger* (LOV-2004-03-05-12).

Barnehageloven. (2005). *Lov om barnehager* (LOV-2005-06-17-64).

Markedsføringsloven. (2009). *Lov om kontroll med markedsføring og avtalevilkår* (LOV-2009-01-09-2).

Politiregisterloven. (2010). *Lov om behandling av opplysninger i politiet og påtalemyndigheten* (LOV-2010-05-28-16).

Skatteforvaltningsloven. (2016). *Lov om skatteforvaltning*, (LOV-2016-05-27-14).

Personopplysningsloven. (2018). *Lov om behandling av personopplysninger* (LOV-2018-06-15-38). Lov 10. juni 2022 nr. 39 om endringer i friskolelova (nytt navn på loven og oppheving av to godkjenningsgrunnlag).

Forskrifter:

Politiregisterforskriften. (2013). *Forskrift om behandling av opplysninger i politiet og påtalemyndigheten* (FOR-2019-09-20-1097).

Kommunikasjonskontrollforskriften. (2016). *Forskrift om kommunikasjonskontroll, romavlytting og dataavlesing* (FOR-2016-09-09-1047).

Forskrift om rammeplan for barnehagens innhold og oppgaver. (2017). *Forskrift om rammeplan for barnehagens innhold og oppgaver* (FOR-2017-04-24-487).

eForvaltningsforskriften. (2020). *Forskrift om elektronisk kommunikasjon med og i forvaltningen* (FOR-2020-10-16-2063).

Traktater:

Menneskerettighetserklæringen. (1948). *United Nations General Assembly, Universal Declaration of Human Rights* (10-12-1948).

Menneskerettskonvensjonen. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms* (04-11-1950)

FN-konvensjonen. (1966). *United Nations General Assembly, International Covenant on Civil and Political Rights* (16-12-1966).

Konvensjon om personvern i forbindelse med elektronisk databehandling av personopplysninger. (1981). *Convention for the Protection of Individuals with regard to the Automatic Processing for Personal Data* (28-01-1981). (CETS no. 108)

Barnekonvensjonen. (1989). *United Nations Convention on the rights of the child* (20-11-1989), (entered into force 2. September 1990) Treaty Series, vol 1577, p 3,

EU-charter om grunnleggende rettigheter. (2000). *Charter of Fundamental Rights of the European Union* (07-12-2000).

Lisboa-traktaten. (2007). *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community* (13-12-2007).

Direktiver:

Personverndirektivet (opphevet). (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (24-10-1995).

Handelspraksisdirektivet. (2005) *Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council* (11-05-2005)

Betalingstjenestedirektivet. (2015). *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC* (25-11-2015).

Politidirektivet. (2016). *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA* (05-05-2016).

Forordninger:

Generell personvernforordning. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC* (27-04-2016)

Utenlandsk lovgivning:

Danmark:

Skattekontrolloven. (2017). *Lov om skattekontroll nr 1535 af 19/12/2017*. (AN013212).
Lovforslag nr. L 73 Folketinget. (2021–2022). *Forslag til Lov om ændring af lov om et indkomstregister, skatteindberetningsloven og skattekontrolloven*. (AN013102)

Sverige:

Datalag. (1973). *Lag om tillsyn över personregister* (SFS 1973:289)

Rettsavgjørelser:

Høyesterettsdommer

Rt. 2014 side 1105
Rt. 2015 side 93
HR-2019-1226-A
HR-2019-2038-A
HR-2021-2403-A

Lagmannsrettsdommer

LB-2017-150679

EU-Domstolen

C-311/18 (Schrems II)

Avgjørelser fra Den Europeiske menneskerettsdomstolen (EMD)

Sunday Times v. The United Kingdom, [J], no. 6538/74, (1980)
Niemietz v. Germany, [J], no.13710/88, (1992)
Schmidt v. Germany, [J], no. 13580/88, (1994)
von Hannover v. Germany, [J] no. 59320/00 (2004)
Glass v. the United Kingdom, [J], no. 61827/00, (2004)
Fadeyeva v. Russia, [J], no. 55723/00, (2005)
Jalloh v. Germany [GC], no. 54810/00, (2006)
Çiçek and Others v. Turkey (dec.), [J] nos. 74069/01, 74703/01, 76380/01, 16809/02, 25710/02, 25714/02 and 30383/02, (2007)
S. and Marper v. The United Kingdom [GC], no.30562/04 and no. 30566/04, (2008)
E.S. and Others v. Slovakia, [J] no. 8227/04, (2009)
Ternovszky v. Hungary, [J] no. 67545/09, (2010)
S.H. and Others v. Austria [GC], no. 57813/00, (2011)
Knecht v. Romania, [J] no. 10048/10, (2012)
Milićević v. Montenegro, [J], no. 27821/16, (2018)
Saber v. Norway [J], no. 459/18, (2020)

Avgjørelser fra Europakommisjonen:

Kommisjonens avgjørelse (EU) 2016/1250. (2016). *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176)*. CELEX 32016D1250

Retningslinjer og forslag:

Europakommisjonen:

Kommisjonens forslag COM/2021/206 final. (2021). *Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.* CELEX 52021PC0206
Forslag til europaparlaments- og rådsforordning om åpne og rettferdige markeder i den digitale sektoren (DMA). (2020). *Proposal for a regulation of the European Parliament and the Council on contestable and fair markets in the digital sector (Digital Markets Act)*. CELEX 52020PC0842
Forslag til europaparlaments- og rådsforordning om europeisk datastyring (Data Governance Act) (2022). *Proposal for a regulation of the European Parliament and the Council on European data governance (Data Governance Act)*. CELEX 52020PC0767

FNs komité for barns rettigheter:

Committee on the Rights of the Children. (2013). *General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)*

Committee on the Rights of the Children. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment.* Convention on the Rights of the Child.

Article 29 Data Protection Working Party:

Article 29 Working Party. (2018). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.*

Article 29 Data Protection Working Party. (2010). *Opinion 2/2010 on online behavioural advertising.*

Det europeiske personvernrådet:

European Data Protection Board. (2020). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.*

European Data Protection Board. (2020). *Guidelines 5/2020 on consent under Regulation 2016/679.*

Litteratur, artikler, tidsskrifter:

Aalen, I. (2019). *Sosiale Medier*. Fagbokforlaget.

Access Now. (2021, 30. november). *The EU needs an Artificial Intelligence Act that protects fundamental rights.*

Aftenposten. (2018, 23. januar). *Nå skal algoritmer og analyser av «big data» avgjøre hvem som blir sjekket ekstra nøye i tollen.*

Algoritmer, Data & Demokrati. (u.å.). *ADD-prosjektet.*

Altinn utvikling. (u.å.). *Samtykkebasert lånesøknad.*

Amnesty International. (2019, 21. november). *Surveillance giants: How the business model of Google and Facebook threatens human rights.*

Andreou, A., Venkatadri, G., Goga, O., Gummadi, K.P., Loiseau, P., Mislove, A. (2018). Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations. *NDSS 2018 – Network and Distributed System Security Symposium,* 1-15.

ANEC. (u.å). *The Standardisation Regulation.*

Arbeids- og velferdsdirektoratet. (2022). *Tildelingsbrev til Arbeids- og velferdsdirektoratet for 2022.*

Arunesh Mathur, A., Mayer, J. & Kshirsagar, M. (2021). What Makes a Dark Pattern… Dark?: Design Attributes, Normative Considerations, and Measurement Methods. *CHI Conference on Human Factors in Computing Systems (CHI '21).*

Authority for Consumers & Markets. (2020, 11. februar). *Consumer better protected against misleading practices online.*

Autoriteit Persoongegevens. (2021). *Tax Administration fined for discriminatory and unlawful data processing.*

Barneombudet. (2017). *Barneombudets supplerende rapport til FNs barnekomité: Barns rettigheter i Norge – 2017.*

Barneombudet. (2019). *Ungdom om digitale medier. Vurderinger og forslag fra Barneombudets ekspertgruppe om en tryggere digital hverdag.*

Barne- og familedepartementet. (2021). *Rett på nett – Nasjonal strategi for trygg digital oppvekst.*

BBC. (2018, 4. juli). *Social media apps are 'deliberately' addictive to users.*

BBC. (2022, 20. januar). *Apple AirTags – A perfect tool for stalking.*

BEUC. (2021). *TikTok without filters.*

Bioteknologirådet (2021, 20. oktober). *Datatilsynet vil ha klare begrensninger på politiets bruk av DNA.*

Bits. (u.å.). *Oppgjør etter dødsfall.*

Bouvet. (2021). *Digitalisering i skolen. Har vi glemt personvernet?*

Breton, T. (2021, 16. september). *How a European Cyber Resilience Act will help protect Europe.* Europakommisjonen.

Brignull, H. (u.å.). *What is deceptive design?*

Brooke Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar & M., Turner, E. (2019). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.* Pew Research Centre.

Bruce, I. & Haugland, G.S. (2014). *Skjulte tvangsmidler.*Universitetsforlaget.

Brønnøysundsregistrene. (2021). *Enklere deling av tilsynsdata med Tilda.*

Bundeskartellamt. (2019, 7. februar). *Bundeskartellamt prohibits Facebook from combining user data from different sources.*

Busse, J. (2022, 10. januar). *Ny lov giver Skat indsigt i, hvor meget du satte din kaffemaskine til salg for på Den Blå Avis.* Alltinget.

Burton-Harris, V. & Mayor, P. (2020, 24. juni). *Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart.* ACLU.

BusinessInsider. (2020, 11. november). *Amazon, Google, and Alibaba face anticompetitive investigations from governments in the EU, China, and India.*

BuzzFeed. (2021, 25. august). *Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here*.

Cavoukian, A. (2009). *Privacy by Design: The 7 Foundational Principles*.

CBC. (2017, 24. november). *How companies use personal data to charge different people different prices for the same produc*t.

Chicago Tribune. (2020, 25. januar). *For years Chicago police rated the risk of tens of thousands being caught up in violence. That controversial effort has quietly been ended.*

Christl, W. (2017, 2. juni). *Corporate Surveillance in Everyday Life*. Cracked Labs.

Christl, W. (2017). *How Companies Use Personal Data Against People*. Cracked Labs.

Christl. W./Cracked Labs. (2022). *Digital Profiling in the Online Gambling Indus*try. Clean Up Gambling.

Cnet. (2019, 14. februar). *These Android apps have been tracking you, even when you say stop*.

Coalition Against Stalkerware. (u.å). *What is stalkerware.*

Dagbladet. (2017, 16. mai). *Reklameskilt ser hvem du er*. DinSide.

Dahlum, S. & Grønmo, S. (2021). *Kausalitet*. Store norske leksikon.

Dataetisk Råd (u.å.). *Om Dataetisk Råd.*

Datatilsynet. (2014). *Årsmelding for 2014.*

Datatilsynet & Teknologirådet. (2015). *Personvern 2015 – Tilstand og trender.*

Datatilsynet. (2015). *Det store datakappløpet.*

Datatilsynet. (2015). *Anonymisering av personopplysninger.*

Datatilsynet. (2016). *Sporing i det offentlige rom*.

Datatilsynet. (2018). *Personlige finanser. Hvordan utviklingstrekk i finanssektoren påvirker personvernet.*

Datatilsynet. (2018). *Om politiregisterloven*.

Datatilsynet. (2018). *Høringsuttalelse – Register over drap og vold med dødelig utgang*

Datatilsynet. (2019). *Programvareutvikling med innebygd personvern*

Datatilsynet. (2019). *På parti med teknologien: Digital målretting av politiske budskap i Norge*.

Datatilsynet. (2019). *Høringsuttalelse – Forslag til ny lov om etterretningstjenesten.*

Datatilsynet. (2020). *I beste mening: Bilder av barn på nett*

Datatilsynet. (2020). *Varsel om irettesettelse for feil bruk av Googles løsninger i skolen.*

Datatilsynet. (2020). *Bruk av Google Chromebook og G Suite for Education (og andre skytjenester) i grunnskolen*

Datatilsynet. (2020). *Personvernombudsundersøkelsen 2020/21.*

Datatilsynet. (2020). *Personvernundersøkelsen 2019/2020.*

Datatilsynet. (2020, 10. juli). *Endelig vedtak om gebyr til Rælingen kommune.*

Datatilsynet. (2021, 16. juli). *Lukker IB-saken.*

Datatilsynet. (2020, 9. september). *Endelig vedtak om gebyr til Bergen kommune.*

Datatilsynet. (2021, 22. september). *Datatilsynet velger å ikke bruke Facebook*.

Datatilsynet. (2021). *Overføring av personopplysninger ut av EØS*.

Datatilsynet. (2021). *Årsrapport for 2020.*

Datatilsynet. (2021). *Overføring av personopplysninger ut av EØS*.

Datatilsynet. (2021). *Vedtak om pålegg til Kriminalomsorgsdirektoratet.*

Datatilsynet. (2022). *Overtredelsesgebyr til Østre Toten kommune*.

Datatilsynet. (2022). *Sandkassesiden*.

Datatilsynet. (2022). *Sluttrapport fra sandkasseprosjektet med KS, SLATE ved UiB og Utdanningsetaten i Oslo kommune. Temaer: Rettslig grunnlag, personvernkonsekvensvurdering (DPIA) og åpenhet.*

Datatilsynet. (2022). *Innebygd personvern og personvern som standard.*

Datatilsynet. (2022). *Årsrapport for 2021.*

Datatilsynet. (2022, 1. mars). *Miniseminar og prisutdeling – Innebygd personvern i praksis 2021.*

Datatilsynet. (2022, 17. mars). *Høring i EU-parlamentet*.

Datatilsynet. (2022, 25. april). *Samtykke fra mindreårige*.

Datatilsynet. (2022). *Høringssvar om EOS-utvalgets behandling av personopplysninger.*

Digitaliseringsdirektoratet (2015, 25. mai). *Advarer mot politiets drøm om bakdør.*

Digitaliseringsdirektoratet. (u.å). *Hel eller delvis automatisering?*.

Digitaliseringsdirektoratet. (u.å.). *Design*.

Digitaliseringsdirektoratet. (u.å). *Datamaskiners muligheter og begrensninger ved automatisert rettsanvendelse.*

Digitaliseringsdirektoratet. (u.å). *Skjønn gjør automatisering vanskelig.*

Digitaliseringsdirektoratet. (u.å). *Koordinering av arbeidet med Schrems II-dommen*.

Digitaliseringsdirektoratet. (u.å.). *Nettverk for informasjonssikkerhet – NIFS.*

Digitaliseringsdirektoratet. (u.å.). *Personvern på Facebook*.

Digitaliseringsdirektoratet. (u.å). *Fordeling av roller og ansvar når dere skal dele data*.

Digitaliseringsdirektoratet. (2022). *Innsynsløsning – tekniske og juridiske muligheter. En utredning av løsninger for å sikre at innbyggerne får innsyn og kontroll over egne personopplysninger.*

Direktoratet for forvaltning og økonomistyring (DFØ). (2021). *Innbyggerundersøkelsen 2021.*

Direktoratet for e-helse. (2019). *Strategi for Normen, 2019-2020.*

Direktoratet for e-helse. (2020). *Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.*

Draper, N.D. & Turow, J. (2019). The corporate cultivation of digital resignation. *SAGE Journals.*

DW. (2022, 18. mars). *Fact check: The deepfakes in the disinformation war between Russia and Ukraine.*

Electronic Frontier Foundation (EFF). (u.å.). *Privacy Badger is a browser extension that automatically learns to block invisible trackers.*

Electronic Frontier Foundation (EFF). (2022). *Surveillance self-defence.*

Engh, I.B. & Blyverket, I.L. (2022, 30. januar). *Barneromsdøren står åpen for kommersielle aktører.* Dagens Næringsliv.

Ericson, I.S. (2022). *Barns samtykkekompetanse på personvernfeltet.* Utredning for Personvernkommisjonen.

Europakommisjonen. (2019). *A definition of Artificial Intelligence: main capabilities and scientific disciplines.*

Europakommisjonen. (2020). *White Paper On Artificial Intelligence: A European approach to excellence and trust.*

Europakommisjonen. (2020). *White Paper on Artificial Intelligence – A European approach to excellence and trust.*

Europakommisjonen. (2020, 17. desember). *Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions.*

Europakommisjonen. (2021, 29. oktober). *Commission strengthens cybersecurity of wireless devices and products.*

Europakommisjonen. (2022). *Regulatory framework proposal on artificial intelligence.*

Europakommisjonen. (2022). *A Europe fit for the digital age.*

Europakommisjonen. (2022). Questions and Answers –New rules to fight child sexual abuse.

Europakommisjonen. (2022, 7. juni). *Online platforms.*

Europaparlamentet. (2022, 20. januar). *Digital Services Act: regulating platforms for a safer online space for users.*

European Court of Human Rights. (2021). *Guide to the Case-Law of the European Court of Human Rights: Data Protection.*

European Data Protection Supervisor. (2020, 5. okotober). *EDPS Decision on the own initiative inquiry on Europol's big data challenge.*

European Data Protection Supervisor. (2021). *Opinion 4/2021: EDPS Opinion on the proposal for amendment of the Europol regulation*

European Data Protection Supervisor. (2021, 23. april). *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary.*

European Digital Rights. (2022, 31. januar). *Secret negotiations about Europol: the big rule of law scandal.*

European Digital Rights. (2022, 11. mai). *Private and secure communications attacked by European Commission's latest proposal.*

Euractiv. (2021, 5. november). *DSA: enforcement for very large online platforms moves toward EU Commission.*Europakommisjonen. (2016). *EU-U.S. Privacy Shield: Frequently Asked Questions.*

EØS-notatbasen. (2021). *Forslag til kommunikasjonsvernforordning.*

Falch, C. (2022). *Rapport til Personvernkommisjonen. Intervjuer med barn og unge om personvern.*

Ferguson, A. G. (2017, 3. oktober). *The police are using computer algorithms to tell if you're a threat.* Time

Financial Times. (2022, 16. februar). *California to adopt UK-style child data law in global push against Big Tech.*

Finansdepartementet. (2016). *Utredningsinstruksen.*

Finansavisen. (2020, 19. august). *Netthandel til himmels under corona.*

FN. (2021). *Menneskerettigheter.*

Forbrukerrådet. (u.å). *Om oss.*

Forbrukerrådet. (u.å). *Tingenes Internett.*

Forbrukerrådet. (2017, 18. oktober). *Elendig sikkerhet i GPS-klokker for barn.*

Forbrukerrådet. (2018). *Every Step You Take.*

Forbrukerrådet. (2018, 5.mai). *Krever trygge IoT-produkter for barn.*

Forbrukerrådet. (2019, 28. februar). *Ung og utsatt for usunn reklame.*

Forbrukerrådet. (2019, 15. mars). *Forbrukere stoler ikke på smarte produkter.*

Forbrukerrådet. (2020). *Out of control.*

Forbrukerrådet. (2021, 14, januar). *Amazon vil ikke gi slipp på kundene.*

Forbrukerrådet. (2021, 22. juni). *International coalition calls for action against surveillance-based advertising.*

Forbrukertilsynet. (u.å.). *Forbrukertilsynets veiledning om handelspraksis overfor barn og unge.*

Forbrukertilsynet og Datatilsynet. (u.å.). *Digitale tjenester og forbrukeres personopplysninger.*

Galperin, E. (2020, 28. februar). *What you need to know about stalkerware*. TedTalks.

Goodwin, T. (2015, 4. mars). *The Battle Is For The Customer Interface*. Techcrunch.

Goodwin, M. (2020). *AI – myten om maskinene*. Humanist Forlag.

Harrison, P. & Gray, C. (2010). The ethical and policy implications of profiling 'vulnerable' customers. *International Journal of Consumer Studies, vol. 34*(4), 437-442.

Heggland, M. (2017). *Barns kontroll over eget personvern gjennom retten til innsyn og samtykke: Styrkes barns rettsstilling ved gjennomføringen av EUs personvernforordning?* [Masteroppgave Universitetet i Oslo]. DUO Vitenarkiv.

Helberger, N., Lynskey, O., Micklitz, H.W., Rott, P., Sax, M. & Strycharz, J. (2021). *EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets*. BEUC.

Helberger, N., Micklitz, H.W. & Rott, P. (2021). *The Regulatory Gap: Consumer Protection in the Digital Economy*. BEUC.

Helse- og omsorgsdepartementet. (2021) *Høringsnotat om endringer i pasientjournalloven*.

Hofstad, K. (2022). Sertifisering. *Store norske leksikon*.

Human Rights Watch. (2017, 22. oktober). *China: Voice Biometric Collection Threatens Privacy.*

Human Rights Watch. (2022). *Students – not products.*

IBM. (u.å.). *What is edge computing?*.

Inc.(2020, 31. juli). *Google Just Revealed How Many People Use Its Privacy Checkup Tool. It's Not Good News.*

Information Commissioner's Office. (2020). *Age appropriate design: a code of practice for online services.*

Integritetsskyddmyndigheten. (2021, 2. oktober). *Beslut efter tillsyn enligt brottsdatalagen – Polismyndighetens användning av Clearview AI.*

International Telecommunication Union. (2015). *Guidelines for Industry on Child Online Protection*.

INTERPOL. (u.å.). *What is INTERPOL?*

Ipsos. (2021). *Sosiale medier tracker Q2'21*.

Irish Council for Civil Liberties. (2020, 21. september). *Two years of DPC inaction on the ongoing RTB data breach: Irish people with AIDS profiled, and Polish elections influenced.*

Irish Council for Civil Liberties. (2021). *Europe's enforcement paralysis. ICCL's 2021 report on the enforcement capacity of data protection authorities*

Irish Council for Civil Liberties. (2022). *The Biggest Data Breach. ICCL report on scale of Real-Time Bidding data broadcasts in the U.S. and Europe.*

Juridika Innsikt. (2021, 9. august). *Smittestopp ble smitteflopp. Har personvern overlevd koronakrise?*.

Justisdepartementet. (2000). *Lovteknikk og lovforberedelse: Veiledning om lov og forskriftsarbeid.*

Justis- og beredskapsdepartementet. (2016). *Høring –endringer i politiregisterloven og politiregisterforskriften –implementering av direktiv (EU) 2016/680.*

Justis- og beredskapsdepartementet. (2018). *Protokoll om endring av Europarådets personvernkonvensjon*.

Justis- og beredskapsdepartementet. (2018). *Høring –utveksling av personopplysninger i forbindelse med bekjempelse av arbeidslivskriminalitet*.

Justis- og beredskapsdepartementet. (2021) *Høring om forslag til forskrift om deling av taushetsbelagte opplysninger og behandling av personopplysninger m.m. i det tverretatlige*
samarbeidet mot arbeidslivskriminalitet

Justis- og beredskapsdepartementet. (2021). *Høring om endringer i straffeloven mv. påvirkningsvirksomhet.*

Justis- og beredskapsdepartementet. (2021). *Høring –endringer i grenseloven mv., ny forskrift om grensetilsyn og grensekontroll av personer (grenseforskriften) mv. og nytt*
kapittel 60 i politiregisterforskriften om behandling av flypassasjerinformasjon (PNR-opplysninger).

Justis- og beredskapsdepartementet. (2021). *Høring – Endringer i politiloven og politiregisterloven mv. – PSTs etterretningsoppdrag og behandling av åpent tilgjengelig*
informasjon.

Justitsministeriet. (u.å.). Dataetisk råd.

Kaufmann, M. (2020). *Likestillingsombudets årskonferanse om kunstig intelligens i et likestillingsperspektiv*. (video)

Kommunal- og distriktsdepartementet. (2019*). Én digital offentlig sektor: Digitaliseringsstrategi for offentlig sektor 2019-2025.*

Kommunal- og distriktsdepartementet & Justis- og beredskapsdepartementet. (2020). *Høring – Endringer i ekomloven.*

Kommunal- og distriktsdepartementet. (2020). *Nasjonal strategi for kunstig intelligens.*

Kommunal- og distriktsdepartementet. (2021). *Hva er fellesløsninger?.*

Kommunal- og distriktsdepartementet. (2021). *Norwegian Position Paper on the European Commission's Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM (2021) 206)*. Europakommisjonen.

Kommunal- og distriktsdepartementet & Barne- og familiedepartementet (2022, 28. februar). *Norge ønsker forbud mot adferdsbasert markedsføring mot barn og unge på nett.*

Kompetanse Norge. (2021). *Befolkningens digitale kompetanse og deltakelse.*

Kon, G. (2018). *Does anyone read privacy notices?* Linklaters.

Kriminalomsorgen. (u.å.). *Personvernerklæring.*

Kripos. (2019). *Seksuell utnyttelse av barn og unge over internett.*

KS. (u.å.). *Verktøykasse plan- og byggesak.*

KS. (2022). *Personopplysninger i skolen.* Utredning for Personvernkommisjonen.

Kultur- og likestillingsdepartementet. (2020). *Ytringsfrihetskommisjonen.*

Kunnskapsdepartementet. (2017). *Framtid, fornyelse og digitalisering. Digitaliseringsstrategi for grunnopplæringen 2017–2021.*

Kunnskapsdepartementet. (2020). *Handlingsplan for digitalisering i grunnopplæringen 2020-2021.*

Laumann, K. & Grytli, D.M. (2021). *Data er det nye oljesølet*. Morgenbladet.

Lintvedt, M. N. (2022). *Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering.* Utredning for Personvernkommisjonen.

Lintvedt, M. N. (2022). Putting a price on data protection infringement, *International Data Privacy Law. 12*(1)

Los Angeles Times. (2020, 8. desember). *The untold story of how the Golden State Killer was found: A covert operation and private DNA.*

Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., et al. (2022). *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation: final report.*

Lutz, C., Hoffmann & C.P., Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany, *SAGE Journals.*

Mathur, A., Acar, G., Friedman, M., Lucherini, L., Mayer, J., Chetty, M., Narayanan, A. (2019). *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites.*

McDonald, A.M. & Cranor, L.F., (2021). The Cost of Reading Privacy olicies. *I/S: A journal of law and policy for the information society, 2021 (01)*.

Mediebedriftenes Landsforening. (2021, 17. november). *Notat vedrørende MBLs posisjon og innspill til det pågående arbeid i EU om regulering av målrettet annonsering.*

Medietilsynet. (2018). *Barn og medier-undersøkelsen 2018. 9-18-åringer om medievaner og opplevelser.*

Medietilsynet. (2020). *Barn og medier 2020.*

Medietilsynet. (2021, 13. juni). *Medietilsynets ansvar og oppgaver.*

Mejias, U. A. & Couldry, N. (2019). Datafication. *Internet Policy Review* 8(4).

Moghaddam, H. M., Acar, G., Burgess, B., Mathur, A., Huang, D. Y., Feamster, N., Felten, E., Mittal, P., Narayanan, A. (2019). *Tracking Ecosystem of Over-the-Top TV Streaming Devices.*

Morgenbladet. (2021, 3. desember). *Slik ble politiets «supervåpen» en 100-millioners fiasko*.

Morgenbladet. (2021, 17. desember). *Overvåkning: Endret loven for å passe til Palantirs programvare*.

Mozilla. (2021). *YouTube Regrets: A crowdsourced investigation into YouTube's recommendation algorithm*.

Nasjonal Sikkerhetsmyndighet. (2022, 28. februar). *Samleside for skytjenester og sikkerhet.*

Nature. (2020, 18. november). *The ethical questions that haunt facial-recognition research.*

Nasjonal kommunikasjonsmyndighet. (2020, 6. mars). *Informasjonskapsler/cookies.*

Nes, C. (2017, 22. desember). *Betal som du lever.* Dagens Næringsliv.

Norges Bank Investment Management. (u.å.). *Investeringene.*

Norges Bank Investment Management. (u.å.). *Ansvarlig forvaltning.*

Norges Domstoler (u.å.). *Personvern i domstolene og Domstoladministrasjonen.*

Norges Domstoler. (u.å.). *Aktørportalen for advokater.*

Norges Domstoler. (2020). *Årsrapport 2020.*

NRK. (2017, 6. januar). *Salget av mobilklokker til barn tok av før jul tross advarsler.*

NRK. (2017, 5. mai). *Tilbyr rimeligere bilforsikring hvis du lar deg overvåke*.

NRK. (2018, 24. april). *Må svare om kontrakter med selskap knyttet til Facebook-skandalen*.

NRK. (2021, 10. januar). *Sensitiv pasientinformasjon kan være på avveie etter dataangrep*.
NRK. (2021, 6. oktober). *Teknologirådet mener mange offentlige aktører bør forlate Facebook*.
NRK Beta. (2021, 17. desember). *«Supervåpen» fra Silicon Valley ga hodebry og millionsprekk for politiet.*
NRK. (2022, 11. mai). *Advarer mot skreddersydd svindel etter datalekkasje.*
OECD. (2019). *Measuring the Digital Transformation*.
OECD. (2022). *Drivers of Trust in Public Institutions in Norway.*
Olerud, K. (2022). Føre-var-prinsippet. *Store norske leksikon*.
Oslo kommune. (u.å.). *Forebygging av rus og kriminalitet.*
P4. (2022, 27. april). *Kritisk til GPS-overvåking av barn*.
Penney, J. (2016). Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal, 31*(1), 117.
Philips, A. M. (2016). Only a click away. DTC genetics for ancestry, health, love…and more: A view of the business and regulatory landscape. *Applied & Translational Genomics 8.*
Policy Department for Economic, Scientific and Quality of Life Policies. (2021). *ArtificiaI Intelligence and public service.*
Politico. (2021, 31. august). *Machines can read your brain. There's little that can stop them*.
Politico. (2021, 6. oktober). *European Parliament calls for a ban on facial recognition*
Politico. (2022, 20. januar). *European Parliament pushes to ban targeted ads based on health, religion or sexual orientation*.
Politiet. (u.å.). *Politiets Personvernerklæring.*
Politiet. (u.å.). *Nasjonalt cyberkrimsenter (NC3)*.
Politiet. (2021). *Politiets trusselvurdering 2021.*
Politidirektoratet. (2018). *Kriminalitetsforebygging som politiets primærstrategi 2018 – 2020: Politiet mot 2025 – delstrategi.*
Politiforum (2018, 8. april). *Selv om en salgsbrosjyre sier at et dataverktøy kan tenke som et menneske, bør man ikke stole på det*.
Politiforum. (2020, 3. april). *Bråstopp for prestisjeprosjekt.*
Press Freedom Institute. (2021, 21. oktober). *Global Encryption Day: Secure communication vital for journalists*.
Privacy Company. (2021). Google mitigates 8 high privacy risks for Workspace for Education.
Privacy Company. (2021). Privacy assessment Google Workspace (G Suite) Enterprise: Dutch government consults Dutch Data Protection Authority on high privacy risks.
Privacy International. (2017). *Case Study: Profiling and Elections – How Political Campaigns Know Our Deepest Secrets.*
Privacy International. (2019, 9, september). *No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data.*
Privacy International. (2020, 6. februar). *Mental health websites don't have to sell your data. Most still do*.
Privacy International. (2020, 20. august). *Explainer: Competition, Data and Interoperability in digital markets.*
Privacy International. (2021, 4. august). *An unhealthy diet of targeted ads: an investigation into how the diet industry exploits our data*.
ProPublica. (2016, 21. oktober). *Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking*.
PWC. (2022). *Understanding algorithmic bias and how to build trust in AI.*
Rett24. (2021, 3. januar). *Riksadvokaten beordrer brems i politiets mobilgjennomganger.*
Rett24. (2021, 30. august). *Regjeringen går videre med den kontroversielle delen av e-tjenesteloven*.
Rett24. (2021, 5. januar). *Tiltroen til myndighetene rett til værs i korona-Norge*.
Riksrevisjonene i Finland, Nederland, Norge, Storbritannia og Tyskland. (2020). *Auditing machine learning algorithms: A white paper for public auditors.*
Ringnes, W. (2022). Kommersiell sporing – nasjonal risiko. *Internasjonal politikk 80(1)*.
Rooney, T. (2010). Trusting children: How do surveillance technologies alter a child's experience of trust, risk and responsibility. *Surveillance and Society, 7*(3/4), 344-355
Rosenberg, T. G., Steinnes, K. K., Storm-Mathisen, A. (2018). *Markedsføring og personvern i sosiale medier – en flermetodisk undersøkelse med barn som medforskere*. Forbruksforskingsinstituttet SIFO, OsloMet.
Rådet for den Europeiske Union. (2021, 10. februar). *Confidentiality of electronic communications: Council agrees its position on ePrivacy rules.*
Samferdselsdepartementet. (2016). Høring – Vegtrafikkloven ny § 43 b – Rett til å behandle personopplysninger –politiets tilgang til personopplysninger i Statens vegvesens registre.
Samuelsen. E. (1972). *Statlige databanker og personlighetsvern*.
Schartum, D.W. & Bygrave, L. A. (2004). *Personvern i informasjonssamfunnet*. Fagbokforlaget.

Schartum, D.W. (2018). *Digitalisering av offentlig forvaltning – Fra lovtekst til programkode.* Fagbokforlaget.

Schartum, D.W. (2020). *Personvernforordningen: en lærebok*. Fagbokforlaget.

Schulz, W. & Hoboken, J. (2016). *Human rights and encryption*. UNESCO Publishing.

Schneier, B. (2017, 18. juli). *Surveillance is the business model of the internet.* OpenDemocracy.

Seneviratne, S., Kolamunna, H. & Seneviratne, A. (2015). A measurement study of tracking in paid mobile applications. *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec)*.

Sivilombudet. (2022, 13. juni). *Sivilombudet forlater Facebook og Instagram*.

Skatteetaten. *Skattekalkulator.*

Slettemeås, D. (2018). *Kunnskapsoppsummeringer til stortingsmelding om forbrukerpolitikk 2018. Forbrukernes digitale hverdag – utvidet versjon.* Forbruksforskningsinstituttet SIFO. OsloMet.

Staksrud, E & Ólafsson, K. (2019). *Tilgang, bruk, risiko og muligheter, Norske barn på Internett, Resultater fra EU Kids Online-undersøkelsen i Norge 2018.*

Statewatch. (2022, 25. januar). *Europol: Council Presidency proposes workaround for illegal data processing*.

Statistisk Sentralbyrå. (2022). *Norsk mediebarometer 2021.*

Statistisk Sentralbyrå. (2021, 20. september). *Netthandelen høyere enn noen gang*.

Steinnes, K.K., Teigen, H.F. & Bugge, A.B. (2019). *Photophop, fillers og falske glansbilder? En studie blant ungdom om kjønn, kropp og markedsføring i sosiale medier.* Forbruksforskningsinstituttet SIFO, OsloMet.

Stortinget. (2011). *Dokument 16 (2011–2012). Rapport til Stortingets presidentskap fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven.*

Stortinget. (2021, 19. mars). *Stortinget utsatt for IT-angrep.*

Stortinget. (2021, 23. april). *Historisk EU-regulering av kunstig intelligens (AI)*.

Svardahl, A. & Aalen, H.K. (2020). *Can default options lead to credit card default? An empirical analysis of the effect of altered default options on credit card repayment behavior in Norway.* [Masteroppgave Norges Handelshøyskole]. NHH Brage.

Søre Sunnmøre IKT. (2022). Om SSIKT.

ScienceNews. (2022, 25. januar). *How AI can identify people even in anonymized datasets.*

Slotten, S. & Wiese Schartum, D. (2021). Selvbetjent rettshjelp. *CompLex 3/2021.*

Statistisk Sentralbyrå. (2021). *Norsk mediebarometer.*

Stensrud, T.I. (2020). *Retten i det digitale Norg*e. *Senter for rettsinformatikk, 1970-2020*. Bergen Fagbokforlaget.

Stortinget. (2021, 17. februar). *Rådets enighet om ePrivacy åpner for datalagring*.

Stousland, C. & Førde, K. H. (2020, 19. oktober). *Privacy Shield kjent ugyldig: Hva nå?* Digi.

Sun, T., Gaut, A., Tang, S., Huang, Y., ElSherief, M., Zhao, J., Mirza, D., Belding, E., Chang, K., Wang, W, Y. (2019). Mitigating Gender Bias in Natural Language Processing: Literature Review. *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*.

Solove, D.J. (2021). The Myth of the Privacy Paradox. *The George Washington Law Review, 89*(1).

Techcrunch. (2017, 27. juni). *Google sued in Europe for $2.4BN in damages over Shopping antitrust case.*

TechCrunch. (2020, 9. desember). *On encryption and counter-terrorism, EU lawmakers say they'll work for 'lawful' data access.*

TechDK Kommissionen. (2020). *Analyse: Uddannelse og tech*.

Teknologirådet. (2017). *Denne gangen er det personlig.*

Teknologirådet. (2018). *Kunstig intelligens – muligheter, utfordringer og en plan for Norge*.

Teknologirådet. (2020). *Ansiktsgjenkjenning og personvern*.

Teknologirådet. (2020, 18. februar). *Når kunstig intelligens går på trynet*. Dagens Næringsliv.

Teknologirådet. (2020, 30. desember). *De viktigste teknologiske gjennombruddene i 2021.*

Teknologirådet. (2021). *Kommersiell sporing i offentlig sektor*

The Atlantic. (2018, 20. mars). *Can You Sue a Robocar?*

The Guardian. (2017, 30. juli). *Palantir: the 'special ops' tech giant that wields as much real-world power as Google.*

The Guardian. (2018, 17. mars). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.*

The Guardian. (2021, 28. april). *Facebook allows advertisers to target children interested in smoking, alcohol and weight loss.*

The Guardian. (2021, 5. september). *Social media giants increase global child safety after UK regulations introduced.*

The Guardian. (2022, 13. februar). *Plans for age checks on porn sites 'a privacy minefield', campaigners warn*.

The Markup. (2021, 20. mai). *Facebook Said It Would Stop Recommending Anti-Vaccine Groups. It Didn't.*

The National Institute of Standards and Technology. (2019). *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software.*

The New York Times. (2021, 20. august). *Catholic Officials on Edge After Reports of Priests Using Grindr.*

The Register. (2021, 16. desember). *Apple quietly deletes details of derided CSAM scanning tech from its Child Safety page without explanation*.

The Verge. (2018, 26. september). *What happens when life insurance companies track fitness data?*.

The Verge. (2021, 24. mai). *Heat Listed*.

The Verge. (2021, 15. desember). *Apple scrubs controversial CSAM detection feature from webpage but says plans haven't changed.*

The Washington Post. (2021, 26. oktober). *A whistleblower's power: Key takeaways from the Facebook Papers.*

The Washington Post. (2022, 8. mars). *Why encryption can be a matter of 'life or death' in Russia, Ukraine*.

Thon, B.E., Blyverket, I.E. & Egenæs, J.P. (2021, 21. oktober). *Nok er nok! Gigantene må tøyles.* Aftenposten.

Thon, B. E. (2018). *Algoritmene må temmes*. Aftenposten.

Thon. B.E. (2018, 29. november). *Digitalt grenseforsvar, Personvernkommisjon og hva som er godt personvern.* Personvernbloggen. Datatilsynet.

Tidemann, A. & Elster, A. C. (2022). *Maskinlæring*. Store norske leksikon.

Tidemann, A. (2020). *Kunstig intelligens*. Store norske leksikon.

Tracking-Free Ads Coalition. (u.å). *Supporters.*

Turow, J., Hennessy, M. & Draper, D. (2015). *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*.

Twetman, H., & Bergmanis-Korats, G. (2021). *Data Brokers and Security*. Riga: NATO Strategic Communications Centre of Excellence.

UK Competition and Markets Authority. (2021). *Algorithms: How they can reduce competition and harm consumers.*

UK Competition and Markets Authority. (2021, 30. november). *CMA directs Facebook to sell Giphy.*

UNESCO. (2015). *World Trends in Freedom of Expression and Media Development: Special Digital Focus 2015.*

UNICRI. (2019). *Artificial intelligence and robotics for law enforcement.*

Utenriksdepartementet (EU-delegasjonen). (2009, 23. mars). *Prüm forenkler DNA-sporing.*

Utenriksdepartementet (Den faste delegasjonen til OECD og UNESCO). (2021, 1. mars). *Et nytt paradigme for tillit til myndighetene*.

Utdanningsdirektoratet. (2019). *Hvordan beskytte barn mot skadelig innhold på nett?*

Utdanningsdirektoratet. (2011). *Reklame i skolen – veileder.*

Utdanningsdirektoratet. (2017). *Rammeverk for grunnleggende ferdigheter.*

Utdanningsdirektoratet. (2017). *Rammeplan for barnehagen.*

Utdanningsdirektoratet. (2020, 5. juni). *Utvikle digital kompetanse i skolen.*

Utdanningsnytt. (2021, 3. januar). *Digital undervisning: – Kan kreve at elevene slår på kameraet.*

Veale, M. & Borgesius, F.Z. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International, 22*(4), 97-112.

Venturebeat. (2021, 11. januar). *Outlandish Stanford facial recognition study claims there are links between facial features and political orientation.*

Version2. (2020, 29. januar). *Gladsaxe-modellen spøger: Nyt AI-projekt skal forudsige mistrivsel hos børn*.

Visma. (u.å.). *Sikre testdata for NAV som ivaretar personvern*.

Vox. (2020, 2. desember). *A surprising number of government agencies buy cellphone location data. Lawmakers want to know why.*

Wessel-Aas, J. (2017). *Digital grenseovervåkning utenfor lovlige grenser*. NRK Beta.

World Economic Forum. (2021, 1. april). *How to tell reality from a deepfake?*

Zetland. (2021, 4. mai). *For fire år siden fik politiet et «supervåben». Her er, hvordan det har transformeret ordensmagten.*

Zuboff, S. (2020). *Overvåkingskapitalismens tidsalder: Kampen for en menneskelig framtid ved maktens nye frontlinje*. Spartacus.

Norges offentlige utredninger 2021

Arbeids- og sosialdepartementet:
NOU 2021: 2 Kompetanse, aktivitet og inntektssikring
NOU 2021: 5 Grunnlaget for inntektsoppgjørene 2021
NOU 2021: 8 Trygd over landegrensene
NOU 2021: 9 Den norske modellen og fremtidens arbeidsliv

Finansdepartementet:
NOU 2021: 1 Endringer i verdipapirhandelloven
NOU 2021: 4 Norge mot 2025
NOU 2021: 7 Trygg og enkel eiendomsmegling
NOU 2021: 10 Ny lov om folkefinansiering av næringsvirksomhet

Helse- og omsorgsdepartementet:
NOU 2021: 11 Selvstyrt er velstyrt

Kommunal- og moderniseringsdepartementet:
NOU 2021: 6 Myndighetenes håndtering av koronapandemien

Kulturdepartementet:
NOU 2021: 3 Barneliv foran, bak og i skjermen

Bestilling av publikasjoner

Departementenes sikkerhets- og serviceorganisasjon
www.publikasjoner.dep.no
Telefon: 22 24 00 00

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Omslagsfoto: Colourbox

Trykk: Departementenes sikkerhets- og serviceorganisasjon – 09/2022