Norges institusjon for menneskerettigheter

Kommunal- og distriktsdepartementet
Kun sendt per e-post: postmottak@kmd.dep.no

Deres referanse: 22/6868
Vår referanse: 2022/169
Dato: 24.02.2023
Publikasjonsnr.: NIM-H-2023-009

Høringsuttalelse – NOU 2022: 11 Ditt personvern – vårt felles ansvar

1. Innledning

Vi viser til Kommunal- og distriktsdepartementets høringsbrev av 14. november 2022 om Personvernkommisjonens utredning NOU 2022: 11 *Ditt personvern – vårt felles ansvar*. Frist for å avgi uttalelse er forlenget til 24. februar.

Norges institusjon for menneskerettigheter (NIM) har som hovedoppgave å fremme og beskytte menneskerettighetene i tråd med Grunnloven, menneskerettsloven og den øvrige lovgivning, internasjonale traktater og folkeretten for øvrig. Vi skal bidra til å styrke gjennomføringen av menneskerettighetene, særlig ved å gi råd og fremme anbefalinger til Stortinget, regjeringen, Sametinget og andre.[1] Høringsuttalelser er et sentralt virkemiddel i dette arbeidet.

De temaene som tas opp i Personvernkommisjonens rapport er av betydning for en rekke menneskerettslige spørsmål. Kommisjonen uttaler at «[k]ritiske refleksjoner forutsetter grunnleggende forståelse av både teknologien og de juridiske problemstillingene, men i bunn og grunn handler det om å forstå og vektlegge menneskerettighetene i møte med teknologi».[2] Det er etter NIMs syn positivt at temaene er gjort til gjenstand for en offentlig utredning.

Personvernkommisjonens rapport er bredt anlagt, og NIM har i høringssvaret valgt ut enkelte temaer som enten reiser særlig sentrale menneskerettslige spørsmål, eller hvor NIM kan bidra med supplering. Dette betyr også at høringssvaret ikke kan anses uttømmende. NIM har for øvrig behandlet flere av rapportens temaer i forbindelse med tidligere høringer og rapporter, som supplerer denne uttalelsen.[3]

[1] Se NIM-loven §§ 1 og 3 første ledd.
[2] NOU 2022: 11 pkt. 1.1.2.
[3] Se f.eks. høringsuttalelse om endringer i etterretningstjenesteloven 27.09.2022, høringsuttalelse om endringer i politiloven og politiregisterloven, PSTs etterretningsoppdrag og behandling av åpent tilgjengelig informasjon 01.01.2022, høringsuttalelse om endringer i straffeloven mv, påvirkningsvirksomhet 23.08.2021, høringsuttalelse om endringer i grenseloven, grenseforskriften og politiregisterloven om behandling av passasjerinformasjon (PNR-opplysninger) 17.06.2021. Se også NIMs rapport *Ny teknologi og menneskerettigheter* tilgjengelig her og Teknologirådet og NIMs rapport *Menneskerettigheter i metaverset* tilgjengelig her.

I NIMs årsmelding for 2021 var en av anbefalingene til Stortinget at:

> «Stortinget bør be regjeringen om at lovforslag som innebærer økt bruk av informasjonsteknologi, følges av grundige konsekvensanalyser som vektlegger menneskerettighetene, særlig retten til privatliv, ikke-diskriminering og ytringsfrihet.»[4]

I kapittel 2 nedenfor gjennomgås noen grunnleggende utgangspunkter for menneskerettslig beskyttelse. I kapittel 3 behandles forslaget om å etablere en ny personvernpolitikk. I de videre kapitlene behandles et utvalg av kommisjonens forslag; om personvern i justissektoren, om barns personvern og om klageordninger mv.

2. Grunnleggende menneskerettslig beskyttelse

Retten til privatliv, familieliv, hjem og korrespondanse følger av blant annet Den europeiske menneskerettskonvensjon (EMK) artikkel 8, FNs konvensjon om sivile og politiske rettigheter (SP) artikkel 17 og Grunnloven § 102. Barn har dessuten et særlig vern etter FNs konvensjon om barnets rettigheter (barnekonvensjonen) artikkel 16.

Ny teknologi utfordrer imidlertid ikke bare personvernet. Selv om personvernet står i en særstilling, kan også ytringsfriheten og diskrimineringsvernet utfordres med utviklingen og anvendelsen av ny teknologi. Ytringsfrihetskommisjonen har i NOU 2022: 9 behandlet mange av de samme fenomenene som Personvernkommisjonen, men da i et ytringsfrihetsperspektiv. Etter omstendighetene kan også andre rettigheter berøres. Dermed er det sentralt at menneskerettslige vurderinger av tiltak eller lovgivning som kan berøre personvernet ikke bare utredes og vurderes med sikte på disse personvernkonsekvensene, men også med sikte på konsekvenser for andre menneskerettigheter.

3. Spørsmål om personvernpolitikk

I høringsbrevet bes det særlig om at høringsinstansene kommenterer hovedanbefalingen om å utarbeide en nasjonal personvernpolitikk.

Kommisjonen peker på at det i dag ikke foreligger en samlet personvernpolitikk. Vurderinger skjer ofte sektorvis, i det som kommisjonen omtaler som «siloer».[5] Kommisjonen viser til at lovarbeid ofte mangler grundige vurderinger av personvern. Ikke minst gjelder det kommisjonens gjennomgang av hjemler for overvåkning og kontroll i rapportens kapittel 7. Kommisjonen peker også på at uheldige virkninger for *andre* menneskerettigheter ikke «fanges opp», slik som «[…]nedkjølingseffekter som utfordrer ytringsfriheten», og at man dermed risikerer at «[…]grunnleggende spørsmål ikke blir drøftet som en del av lovforarbeidet».[6] Slike svakheter beskrives ikke bare ved regelutforming, men også ved tjenesteutførelse og annen praksis.

[4] NIMs årsmelding, Dokument 6 (2021–2022), 29.03.22 s. 44.
[5] NOU 2022: 11 s. 11, 76 og 79.
[6] NOU 2022: 11 s. 99.

NIM forstår forslaget om «personvernpolitikk» slik at det legger til grunn at arbeidet med å beskytte mot brudd på personvernet, og sikre gode og helhetlige vurderinger ved utforming av regelverk, utvikling av tjenester, rutiner og organisatoriske tiltak, må ledes av myndighetene. Personvernpolitikken må omfatte både offentlig og privat sektor. Dette ansvaret forutsetter i sin tur en grunnleggende demokratisk debatt, som det må legges til rette for. Kommisjonen foreslår konkret at regjeringen årlig bør legge frem en personvernpolitisk redegjørelse for Stortinget. Det er gjennomgående i kommisjonens rapport at det bør skje *samlede* vurderinger, noe som trolig nødvendiggjør organisatoriske endringer. En slik politikk kan utkrystallisere overordnede temaer, og komme i tillegg til detaljerte og individfokuserte personvernregler som er lite tilgjengelige for de fleste.

NIM vil fremheve at utarbeidelse av en samlet nasjonal personvernpolitikk kan bidra til å realisere menneskerettighetene bedre. NIM vil understreke viktigheten av slike samlede og grundige vurderinger, uansett hvordan dette praktisk gjennomføres. Ansvaret kan utledes allerede av Grunnloven § 92 om statens myndigheters plikt til å respektere og sikre menneskerettighetene.

NIM er derfor enig i at spørsmål om personvern bør gjøres til gjenstand for bredere demokratisk debatt. Uten en slik samlet debatt og politikk, kan tendensen til at digitalisering skjer på bekostning av personvernet forsterkes.

I tillegg til svakheter ved for eksempel enkeltlover, fremhever kommisjonen at man i dag heller ikke sikrer at de *samlede* virkningene av flere regelendringer eller tiltak hensyntas tilstrekkelig:

> «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 overskue sammenhengen mellom alle de ulike hjemlene og konsekvensene av utvidelsene.»[7]

NIM har fremhevet tilsvarende synspunkter i høringer på justisfeltet, og er av den oppfatning at en samlet politikk kan bidra til bedre vurderinger av samfunnsmessige konsekvenser.[8]

Personvernregelverket er stort og komplisert, og er skrevet i et språk som er vanskelig å forstå, «ikke bare for innbyggere flest, men også for eksperter».[9]

I tillegg kommer at nasjonalt rammeverk er fragmentert, og at mange forskjellige lover kan ha betydning. Dette gjelder for eksempel forbrukeres personvern, som også berøres av blant annet markedsføringslov og forbrukerkjøpslov. Og det gjelder barns personvern som i tillegg til personvernregler påvirkes av eksempelvis barnehagelov, opplæringslov og vergemålslov.

[7] NOU 2022: 11 s. 95.
[8] Personvernkommisjonen gjennomgår flere lovforslag og kritiske merknader fra NIM og andre i NOU 2022: 11 fra s. 97.
[9] NOU 2022: 11 s. 185.

Personvernregler er individorienterte, uoversiktlige og knyttet til komplisert teknologi. Dette gjør det vanskelig både for den enkelte og for samfunnet å skaffe oversikt og innrette seg. En samlet nasjonal politikk kan etter NIMs syn delvis avhjelpe dette. En slik politikk vil nødvendigvis være mer generell og legge større vekt på samlede samfunnsmessige virkninger enn det som er mulig i individuelle tilfeller.

Det er vanskelig å tenke seg anvendelse av et *føre-var-prinsipp*, som kommisjonen anbefaler, uten en samlet personvernpolitikk. Uten en slik politikk blir det også vanskelig å foreta grundige risikovurderinger, som kommisjonen også anbefaler.

Personvernkommisjonen mener at det bør *forskes* mer på samfunnsmessige konsekvenser av overvåkningstiltak i justissektoren.[10] Det anbefales også at det bør forskes mer på personvernfremmende teknologi.[11] NIM er enig i det. Det er etter NIMs syn også en sammenheng mellom mer forskning på samfunnsmessige virkninger, og en personvernpolitikk; en personvernpolitikk kan tydeliggjøre hvilket behov for forskning som foreligger, en slik politikk kan i større grad forsvare bruk av ressurser til forskning, og en samlet politikk vil i større grad kunne nyttiggjøre seg forskning.

En personvernpolitikk vil også gjøre det mer overkommelig å avveie personvernhensyn mot *andre hensyn*, ikke minst ytringsfriheten og diskrimineringsvernet. Gode personvernregler er dels en forutsetning for ytringsfrihet. Det kan imidlertid også være et spenningsforhold mellom ytringsfrihet og personvern, slik som ved spørsmål om medienes ansvar for krenkelser eller mediers eller bloggeres plikt til å slette opplysninger.[12] Prinsippene om ytringsfrihet er preget av brede skjønnsmessige avveininger, mens personvernregler fremgår av detaljrik og komplisert norsk og europeisk lovgivning. Disse regelsettene kan være vanskelige å sammenholde, og få har god oversikt over det hele. En personvernpolitikk kan, på et mer overordnet plan, legge til rette for en bedre demokratisk debatt om disse avveiningene.

NIM har i denne sammenheng ikke spesielle synpunkter på en slik politikks innhold, ut over at et siktemål bør være å tilrettelegge for en samlet og oversiktlig ivaretakelse av de menneskerettighetene som berøres. Dette kommenteres i kommisjonens rapport avsnitt 1.2, hvor det fremheves at en slik politikk bør må ha «særlig oppmerksomhet på sårbare grupper, herunder barn og unge». NIM er enig i det. Det vil være vanskelig å se hvordan for eksempel barns, eldres eller funksjonshemmedes rettigheter ivaretas, uten slik politikk. Uten den oversikt som en samlet politikk må tilstrebe øker risikoen for utilsiktede virkninger av gode tiltak, slik som tiltakende digitalt utenforskap.

NIM mener imidlertid at siktemålet bør være noe videre, og ivareta *menneskerettighetene generelt.* Ytringsfrihet er eksempel på en rettighet som er uløselig forbundet med personvern, og som ikke bare omfatter sårbare grupper.

[10] NOU 2022: 11 s. 99.
[11] NOU 2022: 11 s. 12 og 201.
[12] Se Vidar Strømme og Mathilde Wilhelmsen, *Retten til å bli glemt: Har mediene sletteplikt?*, Juridika 2022.

4. Det teknologiske landskapet og personvern i digital forvaltning

4.1. Innledning

I kommisjonens utredning kapittel 5 gjennomgås det teknologiske landskapet som påvirker personvernet, og i kapittel 6 gjennomgås personvern i digital forvaltning, herunder bruk av kunstig intelligens. Kommisjonen fremmer en rekke anbefalinger, herunder om et forbud mot biometrisk fjernidentifikasjon, samt krav om kartlegging og forholdsmessighetsvurderinger ved bruk av inngripende teknologi.[13]

NIM har i rapporten *Ny teknologi og menneskerettigheter* fremmet en rekke anbefalinger til myndighetene når ny teknologi skal benyttes i offentlig sektor, enten det gjelder i forvaltningen eller i øvrig myndighetsutøvelse.[14] Anbefalingene kan oppsummeres slik:

- Lovforslag som innebærer økt bruk av informasjonsteknologi, må følges av grundige konsekvensanalyser som vektlegger menneskerettighetene, særlig retten til privatliv, ikke-diskriminering og ytringsfrihet.
- Ved innføring av helautonome beslutningssystemer må myndighetene foreta en særlig grundig analyse som kartlegger konsekvensene for menneskerettighetene.

4.2. Inngripende teknologi og forbud mot biometrisk fjernidentifikasjon

Kommisjonen foreslår et forbud mot biometrisk fjernidentifikasjon i offentlige rom.[15] Det er klart at slike systemer har en side både til retten til privatliv og andre rettigheter, slik som potensielt nedkjølende effekter for ytringsfriheten og demonstrasjonsfriheten.[16]

Biometrisk fjernidentifikasjon på offentlig sted er et inngrep i EMK artikkel 8. NIM kjenner ikke til at EMD har tatt direkte eller prinsipielt stilling til slike systemer.[17] Det er likevel grunn til å tro at konvensjonsmessigheten vil avhenge av formålet med systemet,[18] tilgang til og bruk av opplysninger, samt hvilke tekniske og lovgivningsmessige sikkerhetsmekanismer, som rammer inn tiltaket.[19] Dette inkluderer også hvordan data behandles og lagres, og hva de kan brukes til.[20] NIM mener derfor det er særlig viktig at det gjennomføres grundige menneskerettslige vurderinger før slike systemer vurderes innført.[21]

[13] NOU 2022: 11 s. 55.
[14] NIMs rapport *Ny teknologi og menneskerettigheter,* tilgjengelig: her.
[15] NOU 2022: 11 s. 53.
[16] Se eksempelvis FNs menneskerettighetsråd, *Surveillance and human rights Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, tilgjengelig her.
[17] En sak om ansiktsgjenkjenning på offentlig sted er imidlertid henvist til behandling, se *Glukhin v. Russland* (11519/20).
[18] Eksempelvis har staten en menneskerettslig plikt til å ivareta innbyggernes liv og helse.
[19] Se eksempelvis *Big Brother Watch m.fl. v. Storbritannia* (58170/13 62322/14 24960/15) og *Centrum för Rättvisa v. Sverige* (35252/08).
[20] Se f. eks *Peck v. Storbritannia* (44647/98) og *Gaughran v. Storbritannia* (45245/15).
[21] Se for øvrig Europarådets retningslinjer for ansiktsgjenkjenning, tilgjengelig her.

NIM støtter også kommisjonens generelle anbefaling om kartlegging av konsekvenser ved bruk av inngripende teknologi, og at det gjøres grundige vurderinger av om det finnes mindre inngripende veier til målet.[22]

4.3. Bruk av kunstig intelligens i offentlig sektor; risiko og konsekvensanalyser

Norge har en av de mest digitaliserte offentlige sektorene i verden. Vi har en offensiv strategi om digitalisering og bruk av kunstig intelligens i offentlig forvaltning, og stadig mer av myndighetenes samhandling med borgerne preges av ny teknologi. Slik teknologi kan gi borgerne bedre, mer tilpassede og mer treffsikre tjenester. Det kan også være ressursbesparende for det offentlige dersom stadig flere oppgaver kan løses av teknologi og ikke gjennom menneskelig saksbehandling. Samtidig innebærer teknologien også iboende utfordringer for flere menneskerettigheter.

Vernet mot diskriminering er en sentral menneskerettighet, og følger blant annet av FNs konvensjon om sivile og politiske rettigheter (SP), FNs konvensjon om økonomiske og sosiale rettigheter (ØSK), FNs konvensjon mot rasediskriminering, FNs kvinnekonvensjon og FN-konvensjonen om rettigheter til mennesker med nedsatt funksjonsevne (CRPD), i tillegg til EMK artikkel 14. For kunstig intelligens, herunder maskinlæringssystemer, er det en iboende risiko for at vernet mot diskriminering utfordres. Dette kan eksempelvis skje dersom datasettene som blir benyttet er skjeve eller inneholder bias, eksempelvis knyttet til kjønn, nasjonalitet, religion eller hudfarge. Sike bias kan forsterkes i kunstig intelligens- og maskinlæringssystemer, og lede til feilaktige eller diskriminerende resultater. Dette kan være særlig problematisk dersom det er vanskelig eller umulig å ettergå hvordan et system har fattet en gitt anbefaling eller beslutning («*black box*»-systemer). Som kommisjonen peker på, finnes det mange eksempler på at bruk av kunstig intelligens i offentlig sektor har ledet til feilaktige og diskriminerende beslutninger med vidtrekkende konsekvenser i andre land.[23]

Flere internasjonale organer har pekt på risikoen for nettopp diskrimineringsvernet når stadig flere offentlige oppgaver løses ved hjelp av kunstig intelligens og maskinlæring, herunder FN og Europarådet.[24] Risikoen øker jo vanskeligere det er å etterprøve grunnlaget for anbefalingen eller beslutningen.

Også personvernet kan utfordres både ved trening av systemer, og ved anvendelsen av systemer med virkning for enkeltpersoner. Kunstig intelligens kan benyttes til både å analysere, kontrollere, vurdere og predikere innbyggeres atferd, ofte basert på store mengder personopplysninger. Dette gir i seg selv potensiale til å skape mektige verktøy, som kan forskyve maktbalansen mellom stat og borger.

---

[22] NOU 2022: 11 s. 54.

[23] NOU 2022: 11 s. 67. Se også Amnesty internationals rapport *Xenophobic Machines - Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal*, tilgjengelig her.

[24] Se eksempelvis FNs høykommissær for menneskerettigheter, *The right to privacy in the digital age* (A/HRC/48/31), tilgjengelig her, Europarådets resolusjon CM/Rec (2020)1, tilgjengelig her.

Den danske nasjonale institusjonen for menneskerettigheter har publisert en rapport om bruk av kunstig intelligens i offentlig sektor.[25] Rapporten inneholder en grundig analyse av menneskerettslige risikofaktorer, herunder risiko for feil eller ulovlige avgjørelser, personvernspørsmål, fare for diskriminering og rettssikkerhetsutfordringer. Rapporten viser blant annet at det er viktig at det gjennomføres grundige konsekvensanalyser for menneskerettighetene ved anvendelsen av slik teknologi i offentlig sektor.

Konsekvensanalyser kan gjøres på mange måter og inneholde ulike typer vurderinger. I NIMs rapport *Ny teknologi og menneskerettigheter* anbefaler NIM følgende:

> «Ved innføring av helautonome beslutningssystemer må myndighetene foreta en særlig grundig analyse som kartlegger konsekvensene for menneskerettighetene. I slike tilfeller bør konsekvensanalysen som et minimum inneholde følgende elementer:
>
> - **Begrunnelse**: Når myndighetene beslutter å benytte digitale verktøy til beslutningsstøtte eller til autonome beslutningssystemer oppstår en begrunnelsesplikt. Begrunnelsen må inneholde hjemmel og formål, samt egnethet til å oppnå formålet. Den bør også beskrive alternative løsninger.
> - **Algoritmisk innsyn og kontroll**: Systemet må tilfredsstille krav om innsyn og kontroll. Det må være klart hvordan man sikrer datakvalitet, hvordan oversyn og kontroll kan gjøres på en tilfredsstillende måte, samt hvordan data som går ut på dato ikke legges til grunn.
> - **Overprøving**: Systemet må være konstruert på en måte som gjør det mulig å etterprøve beslutningen, samt å utøve kontradiksjon. Når profileringsmodeller benyttes til beslutninger, må det være vilkår om at modellene er i stand til å produsere konkrete begrunnelser. Det samme vil gjelde profileringsmodeller til beslutningsstøtte.
> - **Kartlegging av risiko for menneskerettighetene**: Myndighetene må kartlegge risikoen for menneskerettighetene, herunder risiko for vilkårlige beslutninger, diskriminerende beslutninger, om teknologien tilfredsstiller GDPRs vilkår om personvern, dataminimering eller om den baserer seg på korrekte data. Kartleggingen bør beskrive hvilke tiltak som kan iverksettes for å begrense slik risiko. Jo mer inngripende tiltak autonome beslutningssystemer muliggjør, desto strengere vilkår stilles til kartlegging av de menneskerettslige konsekvensene og tiltak for å bøte på dette.
> - **Deltakelse for utsatte grupper**: Statlige myndigheter har et særlig ansvar for å sørge for etterlevelse av konvensjonsforpliktelsene under saksbehandlingen. Ved bruk av profileringsmodeller for saksbehandling, må man sikre reelle muligheter for at de berørte kan bli hørt. Ved helautomatiserte prosesser, må det klargjøres hvordan disse rammer sårbare grupper og hvilke tiltak som kan virke avbøtende. Ved bruk av

[25] Institut for Menneskerettigheders rapport *Når algoritmer sagsbehandler,* tilgjengelig her.

beslutningsstøtte, må man sikre at modellen ikke får en uforholdsmessig stor innflytelse og blir beslutningsstyrende istedenfor beslutningstøttende.»

NIM vil også understreke, slik kommisjonen også er inne på, at EMK og andre menneskerettsinstrumenter kan stille ytterligere og strengere krav til vilkår for innsamling og bruk av personopplysninger enn GDPR. NIM støtter i forlengelsen av dette også anbefalingen om at lovregulering av bruk av kunstig intelligens bør motvirke maktubalansen mellom offentlig forvaltning og innbyggere, og at det bør stilles strengere krav til åpenhet og rettssikkerhetsmekanismer jo mer inngripende behandlingen er.

I kommisjonens utredning er anbefalingen om konsekvensanalyser begrenset til tilfeller der slike systemer kan ha «betydelig innvirkning på innbyggernes liv.»[26] NIM mener imidlertid at konsekvensvurderinger bør foretas i alle tilfeller der slike systemer kan ha en innvirkning på menneskerettighetene. «Betydelig» er et uklart inntrykk, og en slik begrensning kan åpne for en gradvis svekkelse av menneskerettighetene over tid.

NIM deler videre kommisjonens bekymring for profilering til kontrollformål.[27] Dette reiser særlige spørsmål knyttet til både nedkjølingseffekter, diskrimineringsvernet, personvernet og rettsikkerhetsgarantier.

4.4. Mangelfulle vurderinger av personvernkonsekvenser i lov- og forskriftsarbeider

Personvernkommisjonen peker på at det er tydelige mangler ved vurderinger av personvernkonsekvenser i lov- og forskriftsarbeider.[28] NIM deler denne oppfatningen, som påpekt blant annet i vårt høringssvar til lovforslag om å gi PST mulighet til å behandle åpent tilgjengelig informasjon[29], og til etterretningstjenesteloven.[30] I mange inngripende lovforslag fremkommer det ikke tydelig hvordan forholdet til menneskerettighetene er vurdert, eller hvorfor de positive konsekvensene av inngrepet veier opp for de menneskerettslige implikasjonene. Da vanskeliggjøres også reell demokratisk debatt om forslagene.

NIM er også som kommisjonen bekymret for om ulike tiltak, særlig i justissektoren, i for liten grad sees i sammenheng. De samlede effekter både for individ og samfunn får dermed for liten oppmerksomhet, se også nedenfor i avsnitt 5 om personvern i justissektoren, samt våre innledende bemerkninger om en samlet personvernpolitikk.

Som et tiltak foreslår kommisjonen en ny veileder til utredningsinstruksen om vurderinger av personvernkonsekvenser, samt en oppdatering av veilederen om lovteknikk og lovforberedelse. NIM har over tid anbefalt at kravet til utredning av betydningen for

[26] NOU 2022: 11 s. 85.
[27] NOU 2022: 11 s. 81.
[28] NOU 2022: 11 s. 75 flg.
[29] Høringsuttalelse - Endringer i politiloven og politiregisterloven mv. – PSTs etterretningsoppdrag og behandling av åpent tilgjengelig informasjon, tilgjengelig her.
[30] Høringsuttalelse - Endringer i etterretningstjenesteloven, tilgengelig her.

menneskerettighetene *generelt* bør fremgå eksplisitt av utredningsinstruksen.[31] NIM har også et pågående arbeid om en veileder til utredning av menneskerettslige problemstillinger.

I årsmeldingen for 2021 anbefalte NIM at Stortinget bør be regjeringen om at lovforslag som innebærer økt bruk av informasjonsteknologi, baseres på grundige konsekvensanalyser som vektlegger menneskerettighetene, særlig retten til privatliv, ikke-diskriminering og ytringsfrihet.[32] Anbefalingene er som nevnt også utdypet i rapporten *Ny teknologi og menneskerettigheter*.[33] Etter NIMs syn bør slike analyser også inneholde noe om de samlede effektene av foreslåtte tiltak i kombinasjon med allerede eksisterende tiltak.

5. Personvern i justissektoren

I utredningens kapittel 7 behandler kommisjonen personvern i justissektoren, som omhandler blant annet politiet, PST, kriminalomsorgen, påtalemyndigheten og domstolene.

Kommisjonen peker på at der personvernet og hensynet til kriminalitetsbekjempelse står i et motsetningsforhold til hverandre, kan ikke utgangspunktet være at personvernet alltid må vike, slik eksempelvis de der siterte forarbeidene til politiloven kan gi inntrykk av.[34] Kommisjonen peker også på at det ofte ikke gjøres reelle forholdsmessighetsvurderinger, og at det ikke foretas noen samlet vurdering av mengden tiltak justissektoren har mulighet til å ta i bruk.[35] Slike forholdsmessighetsvurderinger kan knyttes til selve tiltakene, og også til hvilke kontroll- og rettssikkerhetstiltak som skal vedtas, og grad av åpenhet. NIM deler disse synspunktene, jf. avsnitt 4.4 ovenfor.

Som nevnt har rekke lovforslag de senere årene vært preget av kortfattede eller mangelfulle vurderinger av forholdet til menneskerettighetene. Som kommisjonen peker på er vurderingene ofte også preget de negative konsekvensene for individet, mens konsekvensene for samfunnet som helhet ofte ikke drøftes i særlig grad. Dersom mangelfulle utredninger kombineres med en grunnholdning om at hensynet til kriminalitetsbekjempelse som utgangspunkt har forrang, vil det i realiteten være lite som står i veien for iverksettelsen av stadig nye og inngripende kontrolltiltak overfor befolkningen.

Kommisjonen foreslår at det bevilges midler til forskning på samfunnsmessige konsekvenser av overvåkingstiltak i justissektoren. NIM støtter dette. Der konsekvensene av et gitt tiltak er ukjente eller usikre, vil forholdsmessighetsvurderingen som skal gjøres etter blant annet EMK artikkel 8 være vanskelig å foreta. Ved nye teknologiske

[31] NIMs årsmelding for 2016, s. 20-21 og NIMs årsmelding for 2017, s. 20-21. Se også NIMs brev av 25. juni 2021, tilgjengelig her, NIMs brev av 2. februar 2023, tilgjengelig her, samt kronikk av Kirsten Kolstad Kvalø og Mathilde Wilhelmsen, *Vi risikerer å bryte menneskerettighetene ved et arbeidsuhell*, Morgenbladet 3. februar 2022, tilgjengelig her.

[32] NIMs årsmelding for 2021, s. 44-45

[33] NIMs rapport *Ny teknologi og menneskerettigheter,* kapittel 8.

[34] NOU 2022: 11 s. 88.

[35] NOU 2022: 11 s. 96 og 87.

hjelpemidler vil det ofte være regelen heller enn unntaket at det er vanskelig å overskue de menneskerettslige konsekvensene, både for individer og for samfunnet som helhet. Etter NIMs syn bør derfor slike lovforslag ledsages av forskning som kan kartlegge og evaluere de samfunnsmessige konsekvensene, også etter at lovforslaget er vedtatt. På denne måten kan man få et bedre grunnlag for å vurdere de menneskerettslige implikasjonene, og eventuelt gjøre nødvendige lovendringer eller iverksette kompenserende tiltak.

Personvernkommisjonen anbefaler også at metodebruk i justissektoren utredes, herunder personvernkonsekvenser av politiets metoder.[36] NIM støtter også dette forslaget. Allerede i 2009 pekte Metodekontrollutvalget i sin evaluering på utfordringer som gjorde det vanskelig å kartlegge bruken av og betydningen av inngripende metoder slik som skjulte tvangsmidler.[37] Teknologien har utviklet seg vesentlig siden den gang, og vil sannsynligvis innebære nye muligheter for kriminalitetsbekjempelse også i fremtiden. NIM mener det bør vurderes om også tollvesenets metodebruk bør inngå i en slik utredning.

Også rettspraksis har avdekket svakheter. I 2020 ble Norge dømt i EMD for brudd på EMK artikkel 8 i en sak om speilkopiering av en siktets mobiltelefon som inneholdt advokatkorrespondanse.[38] Datatilsynet har også nylig bedt om en redegjørelse fra Oslo politidistrikt etter et varsel om at etaten ikke har tilstrekkelig kontroll over digitale beslag. Datatilsynet har blant annet bedt om svar på hvordan bevisene er håndtert med tanke på konfidensialitet, sikkerhetstiltak og sporbarhet. Politiet har selv pekt på omfattende svakheter knyttet til håndteringen av slike beslag.[39]

NIM deler dessuten bekymringen for om ulike tiltak, særlig i justissektoren, i for liten grad sees i sammenheng. De samlede effekter både for individ og samfunn får for liten oppmerksomhet når ulike tiltak kun vurderes isolert. Datatilsynet har eksempelvis uttalt at det samlede overvåkingstrykket nå innebærer en for høy risiko for den enkeltes frihet.[40]

Kommisjonen er også bekymret for formålsutgliding, herunder at innsamlet informasjon benyttes til andre formål enn de opprinnelig er innhentet for. NIM understreker at annen bruk også må tilfredsstille krav til lovhjemmel, formålstjenlighet og forholdsmessighet, og støtter kommisjonens anbefalinger om å etablere både organisatoriske og tekniske tiltak for å forhindre urettmessig bruk av slike opplysninger.

6. Barns personvern

6.1. Innledning – om grunnlaget for utredningen

Barns personvern er særlig omtalt i punkt 2.3 i mandatet til Personvernkommisjonen, og er omtalt flere steder i utredningen.

[36] NOU 2022: 11 s. 104.
[37] Se eksempelvis NOU 2009: 15 s. 114.
[38] *Saber v. Norge* (495/18).
[39] Artikkel i Dagens Næringsliv, *Datatilsynet krever svar fra Oslo-politiet etter varsel*, 18.01.23, tilgjengelig her.
[40] Kronikk i Dagsavisen, *Når er det nok overvåking?,* 8.02.23, tilgjengelig her.

NIM vil for det første berømme kommisjonen for å ha innhentet synspunkter fra barn og unge som en del av sin utredning.[41] Medvirkning fra barn og unge i utredningsprosesser bidrar til å realisere deres rettigheter etter barnekonvensjonen artikkel 12, og til et bedre og mer opplyst kunnskapsgrunnlag for vurderingene som skal gjøres og som handler om barn.[42]

For det andre vil NIM trekke frem som positivt at utredningen også behandler barns rettigheter etter Grunnloven og barnekonvensjonen, og redegjør for disse rettighetene både overordnet og som en del av vurderingene. Vi mener imidlertid at det er behov for grundigere utredninger av ulike spørsmål opp mot menneskerettslige krav. Særlig mener vi at utredninger på dette feltet i større grad bør ta utgangspunkt i barnekonvensjonen artikkel 16 om barns rett til privatliv og kravene denne stiller til statene. Som kommisjonen peker på i utredningen, er det lite praksis om denne artikkelen, både nasjonalt og internasjonalt. Det finnes imidlertid rettskilder som kan belyse innholdet i artikkelen nærmere, herunder generell kommentar nummer 25 om barns rettigheter i det digitale miljøet som også kommisjonen viser til. I denne kommentaren gir FNs barnekomité et kortfattet resymé av hvordan inngrepsvurderingene etter artikkel 16 skal foretas:

> *«Interference with a child's privacy is only permissible if it is neither arbitrary nor unlawful. Any such interference should therefore be provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimization, be proportionate and designed to observe the best interests of the child and must not conflict with the provisions, aims or objectives of the Convention».*[43]

I lys av den generelle gjennomføringsforpliktelsen i barnekonvensjonen artikkel 4 gir også artikkel 16 forpliktelser til å treffe andre tiltak.[44] Vi nevner også at artikkel 16 nr. 2 gir en lovgivningsforpliktelse for statene, som med fordel kunne vært nærmere vurdert. Også praksis etter FNs konvensjon om sivile og politiske rettigheter artikkel 17, som artikkel 16 er modellert etter, samt EMK artikkel 8, kunne vært nærmere analysert for å gi bakgrunn for tolkningen av artikkel 16.

I tillegg har FNs barnekomité gitt tilbakemeldinger til Norge om retten til privatliv i avsluttende merknader, noe vi kommer tilbake til nedenfor.

Som nevnt er kommisjonen inne på at det er lite praksis etter barnekonvensjonen artikkel 16. Mangelen på praksis kan tenkes å ha sammenheng med i hvilken grad barn har

[41] Christian G. Falch, *Intervjuer med barn og unge om personvern*, Rapport Personvernkommisjonen- GFC_V12 (regjeringen.no)

[42] NIM har gitt ulike innspill om dette til myndighetene over tid, og har blant annet anbefalt at høring av barn og unge inntas i mandatene til offentlige utvalg som berører barn. Les mer her: Barn og unges medvirkning i politikk og utredninger – hva er greia? - Norges institusjon for menneskerettigheter (nhri.no)

[43] Barnekomiteen, generell kommentar (GC) nr. 25 om barns rettigheter i det digitale miljøet (2021), CRC/C/GC/25, avsn. 69.

[44] Se også Barnekomiteen, generell kommentar nr. 25 avsn. 70, der komiteen skriver at statene «[s]hould take legislative, administrative and other measures to ensure that children's privacy is respected and protected by all organzations and in all environments that process their data (…)».

muligheter til å klage over brudd på rettighetene etter denne artikkelen, som vi kommer tilbake til i punkt 6.7.

6.2. Barns personvernrettigheter i skole og barnehage

Personvernkommisjonen har over et helt kapittel utredet personvernutfordringer i skole og barnehage. Kommisjonen trekker frem dette som et område med mange nye utfordringer, og der det er behov for tiltak.

NIM er enig i kommisjonens analyser og forslag til tiltak på dette området. Dette er et område som til nå har overlatt mye av vurderingene til den enkelte kommune, skole eller til og med lærer. Også kommuner har ansvar for å gjøre selvstendige vurderinger av barns rettigheter, herunder personvernrettigheter, men det er et statlig ansvar å sørge for at kommunene er rustet til dette gjennom nasjonale føringer. Vi støtter derfor tiltak som kan gi kommunene og enhetene mer støtte i dette, inkludert en nasjonal tjenestekatalog.

NIM støtter forslaget om styrking av opplæring i personvern som grunnleggende menneskerettighet i skolen. Vi viser til at FNs barnekomité i generell kommentar nummer 25 peker på både behovet for informasjonsspredning og opplæring.[45]

6.3. Barns forbrukerrettigheter

Personvernkommisjonen har flere forslag som handler om barns rett til personvern i forbrukerrettslig sammenheng.

Kommisjonen anbefaler for det første et eget lovutvalg om temaet beskyttelse av barn i digitale flater. Forslaget er nokså vidt etter sin ordlyd, men synes ut fra konteksten å være vinklet mot de forbrukerrettslige sidene av barns personvern, der barn blir kommersielt utnyttet av kommersielle aktører. NIM støtter en gjennomgang av dette, og viser til at anbefalingen blant annet bygger på innspill fra Forbrukerrådet og Barneombudet. Spørsmålet om hvordan reglene håndheves, herunder hvilke klageordninger som er tilgjengelige for barn som opplever krenkelser, bør være en sentral del av utredningen.

Vi vil imidlertid kort nevne at det også er en rekke andre trusler mot barn på nett, der det kan være grunn til å utrede deres rett til beskyttelse på digitale flater. Ett eksempel er rett til beskyttelse mot hatprat, som har en side til rett til beskyttelse mot ulovlige angrep på ære og omdømme etter barnekonvensjonen artikkel 16, som blant annet er tematisert av Ungdommens Ytringsfrihetsråd.[46] Vi antar at det kan være hensiktsmessig å avgrense forslaget i denne omgang til å omhandle beskyttelse mot kommersiell utnyttelse, eller overtramp fra kommersielle aktører, men vi minner om at retten til beskyttelse også rekker videre, og at det også må vurderes behov for tiltak eller utredninger i andre sammenhenger.

For det andre går hele Personvernkommisjonen inn for forbud mot atferdsbasert markedsføring mot barn. NIM støtter dette forslaget. Vi viser til at FNs barnekomité i

[45] Barnekomiteen, generell kommentar nr. 25 avsn. 32 og 33.

[46] Ungdommens Ytringsfrihetsråd, 2021, se særlig kap. 4.1. Rapporten er tilgjengelig her.

generell kommentar nummer 25 anbefaler at statene «[s]hould prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling (…)».[47]

NIM mener samtidig at det er nødvendig å vurdere behovet for ytterligere regulering av atferdsbasert markedsføring mot barn ut over det som vil følge av Digital Services Act (DSA). Som påpekt av blant andre Forbrukerrådet i deres høringssvar til utredningen, er det ikke alle tilbydere av tjenester som vil være omfattet av forbudet etter DSA. Vi støtter derfor også et forbud mot bruk av barns personopplysninger til atferdsbasert markedsføring.

Personvernkommisjonen uttaler også at barn ikke skal settes i situasjoner hvor de må gi opp retten til personvern for å kunne utøve øvrige rettigheter. Kommisjonen skriver også at 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, og at personvernet ikke må være en hindring for disse rettighetene. NIM er enig i dette, og viser blant annet til barnekomiteens generelle kommentar nummer 25, som sier at «[p]rivacy and data protection legislation and measures should not arbitrarily limit children's other rights, such as their right to freedom of expression or protection».[48]

6.4. Barns rett til personvern i familiære forhold

Personvernkommisjonen gir korte, men gode analyser av utfordringer for barns rett til personvern i familiære forhold. Så vidt vi kan se fremmes det to konkrete anbefalinger: kompetanseheving og undervisning som skal forebygge personvernutfordringer knyttet til innhold som deles av foreldre (og andre), samt en veileder for å styrke forståelsen av barns rett til personvern i familiære forhold, som særlig gjelder foreldres adgang til å overvåke barns internettaktiviteter.

NIM støtter disse forslagene. Vi mener imidlertid at det på dette området også er behov for ytterligere tiltak. Det er nettopp innenfor området barns personvern i familiære forhold at det for tiden er mange uløste spørsmål og pågående debatter. Som nevnt innebærer barnekonvensjonen artikkel 16 forpliktelser til å treffe tiltak for å beskytte personvernet. Statene står nokså fritt i utformingen av tiltak, så lenge tiltakene samlet bidrar til å oppfylle forpliktelsene. NIM har ikke særskilt kompetanse eller mandat til å foreslå konkrete løsninger, men viser til at tiltak på dette området må være kunnskapsbaserte. Vi vil kort adressere noen særlige premisser eller forhold som kan tas i betraktning ved utformingen av tiltak på området.

For det første vil vi peke på at en del av utfordringene her henger delvis sammen med de uløste rettslige problemstillingene knyttet til barns samtykkekompetanse på personvernområdet, som vi vil adressere i neste punkt.

[47] Barnekomiteen, generell kommentar nr. 25, avsn. 42.
[48] Barnekomiteen, generell kommentar nr. 25, avsn. 74.

For det andre er det et viktig poeng er at selv der foreldre har samtykkekompetanse på vegne av barnet, må denne ivareta barnets rett til privatliv etter barnekonvensjonen. Dette tydeliggjøres av Høyesterett i HR-2019-2038-A (publisering av sensitive bilder og videoer av eget barn) for de tilfellene som rammes av straffeloven. Samtykkekompetansen gjør ikke en slik handling straffri. Det er imidlertid uløste problemer for den typen privatlivsinngrep som ikke rammes av straffeloven, som blant annet Barnelovutvalget peker på som bakgrunn for sin foreslåtte bestemmelse i ny barnelov § 6-7. Som vi vil kommentere særskilt under, er det også uløste problemstillinger knyttet til klagemuligheter og håndheving på dette området.

For det tredje vil vi peke på at det bør vurderes i hvilken grad teknologiske løsninger kan bidra til ivaretakelsen av barns rett til personvern på dette området.[49] Til illustrasjon kan det nevnes at Storbritannias nye lovgivning på området, den såkalte Age Appropriate Design Code, som også er omtalt av Personvernkommisjonen, gir noen løsninger som kan vurderes også i norsk lovgivning. Denne lovgivningen stiller krav til plattformtjenestene for ivaretakelse av barns personvern.[50]

6.5. Særlig om personvernrettslig myndighetsalder

Av mandatet til Personvernkommisjonen følger det at kommisjonen skulle utrede barns samtykkekompetanse på personvernfeltet. Personvernkommisjonen har fått en grundig vurdering av dette spørsmålet gjennom den vedlagte eksterne utredningen gjennomført av Ingvild S. Ericson, som går opp både norsk rett og forpliktelsene og skrankene etter internasjonale forpliktelser.

NIM kan imidlertid ikke se at kommisjonen gjør noen nærmere vurderinger av barns samtykkekompetanse på bakgrunn av utredningen.

NIM vil fremheve at fravær av regelverk om barns samtykkekompetanse på personvernområdet gjør rettstilstanden uklar. I dag er det kun aldersgrensen på 13 år for samtykke til personopplysninger i forbindelse med informasjonssamfunnstjenester som gir barnet en samtykkekompetanse, noe som innebærer at barnet generelt ikke selv har personvernrettslig myndighet før det fyller 18 år. Datatilsynet opererte tidligere med veiledende aldersgrenser, som det nå har gått bort fra. Som vist av både Barnelovutvalget, Åpenhetsutvalget og i utredningen som er vedlegg til Personvernkommisjonen, har Datatilsynets tidligere veiledende aldersgrenser imidlertid vært brukt i en rekke sammenhenger og sektorer, for eksempel innen forskning, og i pressens vurdering av behov for samtykke, eller ved vurderingen av hvem som har samtykkekompetanse knyttet til retten til eget bilde etter åndsverkloven.[51]

NIM legger til grunn at det for ivaretakelsen av barns rettigheter på personvernområdet er nødvendig å klargjøre spørsmålet om barns samtykkekompetanse. Vi viser til at det i

[49] Se også Barnekomiteen, generell kommentar nr. 25 avsn. 70, som bl.a. sier at «[s]tates parties should require the integration of privacy-by-design into digital products and services that affect children».

[50] Se https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/

[51] Se nærmere om dette i Ericson, I.S. (2022). *Barns samtykke på personvernfeltet,* utredning for Personvernkommisjonen.

lovgivningen for øvrig er inntatt en rekke særlige hjemler for overgang av samtykkekompetanse fra forelderen til barnet. Ved den nærmere vurderingen av regler om samtykkekompetanse, bør det ses hen til barnekonvensjonen artikkel 5 om barnets gradvise utvikling av evner og anlegg. Se også FNs barnekomités generelle kommentar nr. 25, som stiller krav til selve samtykket, og som implisitt peker på at samtykkekompetansen kan ligge hos enten barnet eller foreldrene avhengig av barnets alder og gradvise utvikling:

> *«Where consent is sought to process a child's data, States parties should ensure that consent is informed and freely given by the child or, depending on the child's age and evolving capacity, by the parent or caregiver, and obtained prior to processing those data (…)».*[52]

Vi vil i denne sammenhengen også peke på at en tydeliggjøring av forholdet mellom barns og foreldres samtykkekompetanse, ikke bør føre til at det innføres krav om foreldresamtykke på områder hvor det ikke er behov for dette. Det er mye som i dag ikke reguleres av en personvernrettslig aldersgrense, og som heller ikke bør gjøre det. I FNs barnekomités generelle kommentar nummer 25 sier barnekomiteen for eksempel at «[p]roviders of preventive or counselling services to children in the digital environment should be exempt from any requirement for a child user to obtain parental consent in order to access such services».[53]

6.6. Klageordninger – «access to justice» for barn på personvernfeltet

Personvernkommisjonen behandler problemstillinger knyttet til veiledning, tilsyn og klage i kapittel 13. Spørsmål om hvordan barns personvernrettigheter kan håndheves i norsk rett, reiser særlige problemstillinger. Dette gjelder både der privatpersoner, inkludert foreldre, har krenket slike rettigheter, og hvor dette skyldes myndighetsinngrep eller handlinger fra andre private aktører.

FNs barnekomité peker i generell kommentar nummer 25 på at barn må gis tilgang til prøving av klager og krenkelser i det digitale miljøet, og til behovet for uavhengige overvåkningsmekanismer.[54] I relasjon til retten til privatliv nevner også barnekonvensjonen at lovgivningen må inkludere «access to remedy».[55]

Personvernkommisjonen er så vidt innom dette i en barnespesifikk kontekst når den peker på at personvernregelverket i dag ikke regulerer 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.

NIM ønsker å kommentere dette spesifikt, og etterlyse videre utredning av dette, av flere årsaker. For det første er det generelle mangler ved barns klageordninger, som NIM har

[52] Barnekomiteen, generell kommentar nr. 25, avsn. 71.
[53] Barnekomiteen, generell kommentar nr. 25, avsn. 78.
[54] Barnekomiteen, generell kommentar nr. 25, pkt. K (avsn. 43 flg.) og F (avsn. 31).
[55] Barnekomiteen, generell kommentar nr. 25, avsn. 70.

fremholdt til myndighetene i flere sammenhenger.[56] For det andre er personvernområdet et område der ulike problemstillinger knyttet til klageadgang kan komme på spissen, som også barnekomiteen har påpekt i flere sammenhenger.[57]

FNs barnekomité ga i 2010 anbefalinger om dette til Norge i de avsluttende merknadene til Norges fjerde rapport:

> *«Protection of privacy*
>
> *The Committee is concerned at information that parents may violate their children's right to privacy when revealing the particulars of their children's lives on webpages, sometimes in order to support positions in custody conflicts.*
>
> *The Committee recommends the State party to mandate the Norwegian Data Inspectorate to prevent parents and others to reveal information about children which violates children's right to privacy and is not in their best interests.»*[58]

Denne anbefalingen ble i sin tid fulgt opp med lovendringer i den gamle personopplysningsloven § 11 tredje ledd, som slo fast at personopplysninger som gjelder barn, ikke skulle behandles på en måte som er uforsvarlig av hensyn til barnets beste. Bestemmelsen ble ikke videreført i den nåværende personopplysningsloven, og departementet pekte den gang på at det kan vurderes å gjøre endringer i enten barneloven eller vergemålsloven.[59] Barnelovutvalget foreslår en generell bestemmelse om barns rett til personvern og privatliv, som også er omtalt av Personvernkommisjonen.

NIM mener imidlertid at ettersom barneloven etter sitt system ikke åpner for overprøving av beslutninger under foreldreansvaret, kan det også være grunn til å vurdere andre regelverk i tillegg til barneloven, for å sikre en reell klagemulighet for barn, og eventuelt andre på barns vegne. Utenom tilfellene som rammes av straffeloven, der § 267 er mest praktisk for disse tilfellene, er det etter gjeldende rett uklart i hvilken grad barn kan få overprøvet sine foreldres beslutninger på personvernområdet der de selv mener at deres privatliv er krenket, for eksempel der foreldre ønsker at barnet skal medvirke i en nyhetsreportasje eller liknende som barnet ikke ønsker. I andre tilfeller kan det være andre som mener at barnets rettigheter ikke er ivaretatt. I begge tilfellene kompliseres dette ved at foreldre i utgangspunktet har samtykkekompetanse på vegne av barnet. Det må likevel vurderes hvor langt foreldresamtykket skal rekke der barnets selvstendige rett til privatliv kommer under press, og hvordan barns rettigheter kan realiseres i disse tilfellene.

---

[56] Se NIMs brev til Familie- og kulturkomiteen på Stortinget, nærmere omtalt her: Behov for styrking av barns klagemuligheter - Norges institusjon for menneskerettigheter (nhri.no)

[57] Foruten tilbakemeldingen til Norge i 2010 kan det også nevnes at barnekomiteen har tatt opp dette med andre stater, se for eksempel avsluttende merknader til Bosnia og Herzegovina, der barnekomiteen «also urges the State party to establish child-specific and child-friendly mechanisms for children to complain against breaches of their privacy (…)», se CRC/C/BIH/CO/2-4 avsn. 38.

[58] Barnekomiteens avsluttende merknader til Norges 4. rapport, avsn. 28 og 29.

[59] Nærmere redegjort for i NOU 2020: 14 pkt. 8.5.7.

NIM viser for øvrig til at Personvernkommisjonen i sin utredning anbefaler at regjeringen arbeider for at ideelle organisasjoner kan få en styrket rolle i å fremme personvern, blant annet gjennom å opptre på vegne av registrerte personer.[60] NIM mener at dette også bør vurderes i lys av barns rettigheter, for å undersøke muligheten for barn for å få prøvet flere saker som gjelder deres rettigheter.

7. Klage, tilsyn, veiledning mv.

I utredningens kapittel 13 gjennomgår Personvernkommisjonen en rekke spørsmål knyttet til tilsyn, klage og veiledning. NIM kan ikke se at utredningen generelt tar for seg retten til effektivt rettsmiddel ved krenkelse av rettigheter etter konvensjonen etter EMK artikkel 13.[61] Den siste tiden har myndighetene sendt på høring flere ulike forslag om overvåkningstiltak.[62] Den teknologiske utviklingen gir nye muligheter for overvåkning og kontroll, som i seg selv kan bidra til å sikre menneskerettigheter eller tungtveiende hensyn, slik som retten til liv, helse og kriminalitetsforebygging. Samtidig innebærer potensialet for overvåkning en risiko for den enkeltes personvern. NIM mener at det bør utredes i hvilken grad de forskjellige gjeldende regelverk er egnet til å sikre den enkelte effektivt rettsmiddel for brudd på retten til privatliv ved myndighetenes tiltak.[63]

Redegjørelsene i utredningens kapittel 13 knytter seg særlig til Datatilsynets mandat og ressurser og til tilsynets kompetanse til å veilede, føre tilsyn og behandle klagesaker etter personopplysningsloven og GDPR. Utvalget trekker frem behovet for en jevnlig styrking av Datatilsynet, samt styrking av kompetansen på personvern hos kompetente myndigheter. NIM viser i denne sammenheng til Datatilsynets høringssvar hvor de trekker frem at de selv av den oppfatning at det ikke lenger er samsvar mellom de oppgavene som de er satt til å løse og de ressursene de har.[64] Det er i så fall bekymringsfullt.

NIM bemerker at effektive kontroll- og rettsikkerhetsmekanismer er sentrale for å ivareta menneskerettslige krav som at inngrep skal begrenses til det som er nødvendig.[65] Personvernkommisjonen skriver:

> «[e]n 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».[66]

[60] NOU 2022: 11, avsn. 10.3.5.

[61] Enkelte steder nevnes adgangen til erstatning for brudd på GDPR, se f.eks. kap. 4.2.3. og domstolskontroll i kap. 7 og 13.7.2.

[62] Se f.eks. 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), Høring - Endringer i politiloven og politiregisterloven mv. – PSTs etterretningsoppdrag og behandling av åpent tilgjengelig informasjon.

[63] Se i denne sammenheng *Rotaru v. Romania* (28341/95) avsnitt 69 der EMD uttaler: «(….) Furthermore, where secret surveillance is concerned, objective supervisory machinery may be sufficient as long as the measures remain secret. It is only once the measures have been divulged that legal remedies must become available to the individual."

[64] Datatilsynets høringsuttalelse av 10.02.22, deres ref. 22/6868

[65] Se f.eks. storkammerdommen *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (931/13) avsn. 137 med videre henvisninger. Se også *Breyer v. Tyskland* (50001/12) avsn. 78.

[66] NOU 2022: 11 pkt. 7.4.4. s. 105.

NIM er enig i dette. Muligheten for kontroll vil både avhenge av personell, men også at vilkårene for behandling av opplysninger er reelt overprøvbare.[67] Videre vil den reelle kontrollen kunne avhenge av at klagemekanismene er tilgjengelige for borgerne.[68] Det er også viktig for å sikre tillit, som igjen kan forhindre eller redusere nedkjølende effekt på f.eks. ytrings-, informasjons og organisasjonsfriheten.[69] Disse aspektene bør være sentrale ved slik forskning som kommisjonen har foreslått, og som NIM har gitt sin tilslutning til.[70]

I utredningens kapittel 7 drøfter kommisjonen behovet for domstolskontroll, og anbefaler det bør vurderes om dagens domstolskontroll av politiets tiltak bør utvides til å omfatte flere tiltak enn i dag. Det er vanskelig å overskue hvilke konsekvenser en slik utvidet domstolskontroll vil kunne ha. Generelt sett kan økt domstolskontroll bidra til å sikre både den enkelte behandlingen av personopplysninger og befolkningens tillit til myndighetene. Som nevnt i pkt. 5 støtter NIM en utredning av politiets metodebruk. Vi mener at en vurdering av rettssikkerhetsmekanismer vil være en viktig del av dette arbeidet.

Så vidt NIM kan se har ikke Personvernkommisjonen vurdert EOS-utvalgets adgang til å føre kontroll med etterretnings-, overvåkings- og sikkerhetstjenestene, eller gitt spesifikke anbefalinger knyttet til EOS-utvalget.[71] NIM vil, som tidligere, fremheve at dersom det vedtas utvidelser av de hemmelige tjenesters mandat og kompetanse til å utøve overvåkningstiltak mot borgerne, er det viktig at tilsynet gis tilstrekkelig med ressurser og kompetanse til å føre kontroll med tjenestene.[72]

I utredningens kapittel 13 gjennomgår Personvernkommisjonen også problemstillinger knyttet til veiledning, herunder Datatilsynets rolle som veileder overfor enkeltindividet, virksomheter og andre interesserte. Personvernkommisjonen trekker i denne forbindelse frem kompleksiteten i og omfanget av personvernregelverket, og skriver at manglende veiledning kan lede til digitalt utenforskap som hindrer muligheten til å delta i det digitale samfunnet.[73]

Ved vurderingen av tiltak som bidrar til å styrke digitaliseringen er det også viktig å sikre at digitaliseringsløsninger ikke virker diskriminerende eller ekskluderende, og at det settes inn avbøtende tiltak for å hindre digitalt utenforskap. Som nevnt i pkt. 6.3. mener NIM at barns personvern må ivaretas i digitale tjenester på en måte som gjør at de kan

[67] Se om dette i pkt. 3 og 4.4. over.
[68] Problemstillingen berøres i NOU 20222:11 pkt. 13.7.2 med henblikk på GDPR art. 77.
[69] Fenomenet beskrives nærmere i NOU 1999: 27 kap. 6.2.3.2.5. s. 121 der den forrige Ytringsfrihetskommisjonen uttaler «[v]år folkerettslige forpliktelse – slik den endres ved Strasbourg-domstolens dynamiske tolkning – kan nok et stykke på vei oppfylles ved utvidelser av rettsstridsreservasjonen. Det er imidlertid bedre å gi en klar regel som kan være forståelig for allmennheten. Uklare regler og/eller vanskelig tilgjengelige prinsipper utviklet av domstolene kan ha en uønsket dempende effekt («chilling effect») på det offentlige ordskiftet.»
[70] Se NOU 2022:11 pkt. 7.5. s. 115, og denne høringsuttalelsens pkt. 3.
[71] EOS-utvalgets rolle nevnes likevel i NOU 2022:11 pkt. 7.1.1. og 7.2.2 og 7.4.8.
[72] Se NIMs høringsuttalelser som nevnt i fotnote 3.
[73] Se NOU 2022:11 pkt. 13.4.3 og 12.4.

utøve andre rettigheter. NIM viser også til myndighetenes forpliktelser etter CRPD.[74] CRPD-komiteen har i generell kommentar nummer 2 uttalt at:

> «New technologies can be used to promote the full and equal participation of persons with disabilities in society, but only if they are designed and produced in a way that ensures their accessibility. New investments, research and production should contribute to eliminating inequality, not creating new barriers».[75]

Ved innføring av nye teknologiske løsninger som pålegges borgerne, må systemer tilpasses ulike gruppers behov slik at deres rettigheter ivaretas.[76]

8. Avslutning

NIM stiller seg til disposisjon for kommentarer og dialog med departementet i den videre behandlingen av saken.

Vennlig hilsen

for Norges institusjon for menneskerettigheter

Gro Nystuen	Mathilde Wilhelmsen
Assisterende direktør	Rådgiver

Dette dokumentet er elektronisk godkjent og har dermed ingen signatur.

[74] CRPD pålegger bl.a. statene å treffe tiltak for å sikre tilgjengelighet (art. 9), ikke-diskriminering (art. 5).
[75] CRPD/C/GC/2 avsn. 22.
[76] Illustrerende er at det i Danmark er vedtatt en rekke obligatoriske selvbetjeningsløsninger, innenfor ulik sektorlovgivning. I Danmark er det nylig sendt på høring forslag om fravikelse fra obligatorisk selvbetjening, som blant annet har mottatt kritikk fra den danske nasjonale institusjon, les mer her: Høringssvar (menneskeret.dk). I høringssvaret er det referert til rapporten *Digital inklusion i det digitaliserede samfund* utarbeidet av fra Digitaliseringsstyrelsen, som er underlagt Finansdepartementet. Rapporten inneholder en innledende analyse av utfordringene for digital inkludering i Danmark i dag. Rapporten er tilgjengelig her: Rapport (digst.dk).